NOTE:
Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.
# Contents

**CONTACTING VEEAM SOFTWARE** ................................................................. 5  
**ABOUT THIS DOCUMENT** ........................................................................... 6  
**INTEGRATION WITH STORAGE SYSTEMS** .................................................. 7  

<table>
<thead>
<tr>
<th>Universal Storage API Integrated Systems .................................................. 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing Storage System Plug-Ins .......................................................... 11</td>
</tr>
<tr>
<td>Update Notifications .................................................................................. 13</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backup Infrastructure for Storage Snapshots .............................................. 14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding VMware vSphere Server ............................................................... 15</td>
</tr>
<tr>
<td>Configuring Backup Proxy ........................................................................ 16</td>
</tr>
<tr>
<td>Enabling HPE 3PAR Web Services API Server ........................................... 18</td>
</tr>
<tr>
<td>Adding Storage Systems ........................................................................... 19</td>
</tr>
<tr>
<td>Rescanning Storage Systems ..................................................................... 65</td>
</tr>
<tr>
<td>Removing Storage Systems ....................................................................... 68</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backup from Storage Snapshots ................................................................. 69</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Data Processing ................................................................................... 70</td>
</tr>
<tr>
<td>Backup from Primary Storage Arrays ....................................................... 72</td>
</tr>
<tr>
<td>Backup from Secondary Storage Arrays .................................................. 76</td>
</tr>
<tr>
<td>Limitation on Number of VMs per Snapshot ............................................. 83</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backup from Cisco HyperFlex Snapshots ................................................... 84</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Modes ...................................................................................... 85</td>
</tr>
<tr>
<td>How Backup from Cisco HyperFlex Snapshots Works ............................... 87</td>
</tr>
<tr>
<td>Configuring Backup Proxies ...................................................................... 88</td>
</tr>
<tr>
<td>Configuring Backup from Cisco HyperFlex Snapshots .............................. 90</td>
</tr>
<tr>
<td>Configuring Direct NFS Access on Cisco HyperFlex (Earlier Than 2.0) ..... 92</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Snapshot Orchestration .............................................................................. 93</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Snapshot-Only Jobs ............................................................. 94</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Backup from Storage Snapshots with Snapshot Retention ....................... 98</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Backup Jobs with Storage Snapshot Retention ..................... 99</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Veeam Explorer for Storage Snapshots ..................................................... 101</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional Restore vs. Restore from Storage Snapshots ....................... 102</td>
</tr>
<tr>
<td>How Restore from Storage Snapshots Works .......................................... 103</td>
</tr>
<tr>
<td>Creating and Deleting Snapshots ............................................................ 104</td>
</tr>
<tr>
<td>Performing Instant VM Recovery ............................................................. 106</td>
</tr>
<tr>
<td>Restoring VM Guest OS Files (Microsoft Windows) ................................ 115</td>
</tr>
<tr>
<td>Restoring VM Guest OS Files (Linux, Unix and Other) ............................ 123</td>
</tr>
<tr>
<td>Restoring Application Items from Microsoft Active Directory ............... 132</td>
</tr>
</tbody>
</table>
Restoring Application Items from Microsoft Exchange ................................................................. 140
Restoring Application Items from Microsoft SharePoint............................................................ 148
Restoring Databases from Microsoft SQL Server ...................................................................... 150
Restoring Databases from Oracle ............................................................................................. 158

ON-DEMAND SANDBOX FOR STORAGE SNAPSHOTS ........................................................................................... 166

REQUIREMENTS AND LIMITATIONS .................................................................................................................. 168
  System Requirements................................................................................................................... 169
  General Limitations .................................................................................................................. 172
  Limitations for Cisco HyperFlex ............................................................................................ 175
  Limitations for Dell EMC VNX, VNXe/Unity ............................................................................ 176
  Limitations for NetApp ............................................................................................................. 177
  Requirements for Universal Storage API Integrated Systems ..................................................... 186

REQUIRED PERMISSIONS .............................................................................................................................. 187
  NetApp Data ONTAP Permissions ............................................................................................. 188
  NetApp SolidFire/HCI Permissions .......................................................................................... 190
Contacting Veeam Software

At Veeam Software we value the feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up to date information about company contacts and offices location, visit www.veeam.com/contacts.html.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com
About This Document

This user guide provides information about integration, main features, and use of Veeam Backup & Replication with storage systems. The document applies to version 9.5 Update 4 and all subsequent versions until it is replaced with a new edition.

Intended Audience

The user guide is intended for anyone who wants to build the data protection and disaster recovery strategy using Veeam Backup & Replication and storage systems that host VM disks. It is primarily aimed at backup administrators, consultants, analysts and any other IT professionals using the product.

Document Revision History

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Date</th>
<th>Change Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 4</td>
<td>7/16/2019</td>
<td>Updated for Veeam Backup &amp; Replication 9.5 Update 4b.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information about Western Digital IntelliFlash storage system integration added:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Universal Storage API Integrated Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requirements for Universal Storage API Integrated Systems</td>
</tr>
<tr>
<td>Revision 3</td>
<td>5/14/2019</td>
<td>Information about Fujitsu ETERNUS storage system integration added:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Universal Storage API Integrated Systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• System Requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requirements for Universal Storage API Integrated Systems</td>
</tr>
<tr>
<td>Revision 2</td>
<td>3/26/2019</td>
<td>Updated for Veeam Backup &amp; Replication 9.5 Update 4a.</td>
</tr>
<tr>
<td>Revision 1</td>
<td>1/22/2019</td>
<td>Initial version of the document for Veeam Backup &amp; Replication 9.5 Update 4.</td>
</tr>
</tbody>
</table>
Integration with Storage Systems

To build the data protection and disaster recovery strategy, you can use capabilities of native snapshots created on production storage systems that host VM disks.

- **Backup from Storage Snapshots.** You can use storage snapshots to create backups and replicas of VMware vSphere VMs hosted on storage systems. Backup from Storage Snapshots speeds up backup and replication operations and reduces the impact of VMware vSphere snapshot removal on the production environment.

- **Veeam Explorer for Storage Snapshots.** You can restore VM data directly from storage snapshots. Veeam Explorer for Storage Snapshots automates the process of VM data recovery and reduces recovery time in 10 times or more.

- **Snapshot Orchestration.** You can configure backup jobs to periodically create storage snapshots on primary and/or secondary storage arrays.

- **Backup from Storage Snapshots with Snapshot Retention.** You can configure backup jobs to create backup files on the backup repository and, additionally, storage snapshots on the primary and/or secondary storage arrays.

- **On-Demand Sandbox for Storage Snapshots.** You can start VMs whose disks are hosted on storage systems in the On-Demand Sandbox. On-Demand Sandbox can be used for testing, training, troubleshooting and so on.

To start working with storage systems, you must properly configure the backup infrastructure. For more information, see Backup Infrastructure for Storage Snapshots. After that, you can use storage snapshots for data protection and disaster recovery operations.

Depending on the storage system type, you can perform the following operations:

<table>
<thead>
<tr>
<th>Operation/Storage</th>
<th>Dell EMC VNX(e)/Unity</th>
<th>HPE 3PAR StoreServ</th>
<th>HPE StoreVirtual</th>
<th>HPE Nimble</th>
<th>NetApp FAS/AFF, FlexArray (V-Series), IBM N series, Lenovo DM-Series</th>
<th>Cisco HyperFlex</th>
<th>IBM Spectrum Virtualize, Lenovo V-Series</th>
<th>Universal Storage API Integrated Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup from Storage Snapshots</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Backup from primary storage arrays</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Backup from secondary storage arrays</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

To start working with storage systems, you must properly configure the backup infrastructure. For more information, see Backup Infrastructure for Storage Snapshots. After that, you can use storage snapshots for data protection and disaster recovery operations.

Depending on the storage system type, you can perform the following operations:
<table>
<thead>
<tr>
<th>Veeam Explorer from Storage Snapshots</th>
<th>✓</th>
<th>✓</th>
<th>✓</th>
<th>✓</th>
<th>✓</th>
<th>x</th>
<th>✓</th>
<th>✓</th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore from primary storage arrays</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restore from secondary storage arrays</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Snapshot Orchestration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapshot-only job for primary storage arrays</td>
<td>✕</td>
<td>✓</td>
<td>✕</td>
<td>✓</td>
<td>✓</td>
<td>✕</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Snapshot-only job for secondary storage arrays</td>
<td>✕</td>
<td>✓*</td>
<td>✕</td>
<td>✓*</td>
<td>✓*</td>
<td>✕</td>
<td>✓*</td>
<td>✕</td>
<td>✕</td>
</tr>
<tr>
<td><strong>Backup from Storage Snapshots with Snapshot Retention</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup job with snapshot retention on primary storage arrays</td>
<td>✕</td>
<td>✓</td>
<td>✕</td>
<td>✓</td>
<td>✓</td>
<td>✕</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Backup job with snapshot retention on secondary storage arrays</td>
<td>✕</td>
<td>✓*</td>
<td>✕</td>
<td>✓*</td>
<td>✓*</td>
<td>✕</td>
<td>✓*</td>
<td>✕</td>
<td>✕</td>
</tr>
<tr>
<td>Other Operations</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓**</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>-----</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>Storage rescan</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓**</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>Snapshot creation and deletion</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>(manual)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

* Storage snapshot technology:
  - **HPE 3PAR StoreServ**: snapshot creation on Peer Persistent target
  - **HPE Nimble**: snapshot replication
  - **NetApp FAS and AFF Series, IBM N series, and Lenovo DM-Series**: snapshot replication with SnapMirror/SnapVault
  - **IBM Spectrum Virtualize and Lenovo V-Series**: snapshot creation on HyperSwap target

** Infrastructure only
*** Contact vendor to check compatibility and storage system configuration
Universal Storage API Integrated Systems

Veeam Backup & Replication offers built-in integrations with storage systems to help decrease impact on the production environment and significantly improve RPOs. Storage vendors, in turn, can leverage the Veeam Universal Storage API framework to integrate their storage solutions with Veeam Backup & Replication. With this kind of integration, you can use snapshots of Universal Storage API integrated systems to perform backup and restore operations.

The following storage systems are supported:

- Fujitsu ETERNUS DX/AF series
- Huawei OceanStor
- INFINIDAT InfiniBox
- NetApp SolidFire/HCI
- Pure Storage FlashArray
- Western Digital IntelliFlash

To start working with Universal Storage API integrated systems, you must perform the following steps:

1. Download the necessary storage system plug-in from the Veeam Download page.
2. Run the setup wizard to install the plug-in.
3. Configure the backup infrastructure for storage snapshots.

After that, you can use Universal Storage API integrated storage snapshots for data protection and disaster recovery operations.
Installing Storage System Plug-Ins

Before you start working with Universal Storage API integrated systems, make sure you have installed the Universal Storage API integrated system plug-in on the Veeam backup server.

NOTE:
If you connect to the backup server remotely with the Veeam Backup & Replication console, you must install the Universal Storage API integrated system plug-in both on the backup server and the machine where you run the console.

To install a plug-in, perform the following steps:

1. Run the plug-in installation file.
   The latest version of the Universal Storage API integrated system plug-in is available at the Veeam Download page.

2. On the welcome screen of the setup wizard click the Next button to proceed to the configuration of the installation.
3. At the **Terms of Usage** step of the wizard, select **I accept these terms**.

4. At the **Ready to Install the Program** step of the wizard, click **Install** to begin installation.

5. When the installation process completes, click **Finish** to close the wizard.

After you install the plug-in, you must configure the backup infrastructure to be able to use storage system snapshots for data protection. For more information, see **Backup Infrastructure for Storage Snapshots**.
Update Notifications

Veeam Backup & Replication uses update notifications to inform you about new versions of Universal Storage API integrated system plug-ins. When a new version of a plug-in becomes available on the website, Veeam Backup & Replication displays an icon in the system tray. An icon is displayed once a week.

To get a new version of a plug-in, double-click the Veeam Backup & Replication icon in the system tray. Veeam Backup & Replication will open the Veeam Download page where you can download the plug-in.

To install the plug-in, follow the steps described in the Installing Storage System Plug-Ins section.
Backup Infrastructure for Storage Snapshots

Before you start working with storage systems in Veeam Backup & Replication, you must properly configure the backup infrastructure. As part of this process, you must perform the following actions:

1. **Add VMware vSphere server.** You must add to the backup infrastructure a vCenter Server or ESX(i) hosts with VMs whose disks are located on the storage system.

2. **Configure a backup proxy.** The backup proxy is required for storage systems rescan and Backup from Storage Snapshots.

3. **[For HPE 3PAR StoreServ] Enable HPE 3PAR Web Services API server.** Veeam Backup & Replication uses the HPE 3PAR Web Services API server to work with the HPE StoreServ storage system.

4. **Add storage systems.** You must add to the backup infrastructure the storage systems on which VM disks are hosted. If you plan to work with secondary storage arrays, you must add them to the backup infrastructure as well.

5. **[For IBM Spectrum Virtualize with HyperSwap function] If you plan to select secondary storage volumes as a data source for backup, use registry keys.** For more information, contact Veeam Support Team.

NOTE:

You can work with storage systems in the **Storage Infrastructure** view of Veeam Backup & Replication. Right after the installation, the **Storage Infrastructure** view is not displayed in the Veeam Backup & Replication console. To display it, you must add at least one vCenter Server or ESX(i) host to the backup infrastructure.
Adding VMware vSphere Server

Before you add a storage system and start using storage snapshots for backup and restore operations, you must add a VMware vSphere server to the backup infrastructure. The VMware vSphere server is the vCenter Server or ESX(i) host with VMs whose disks are hosted on the storage system. For more information, see Adding VMware vSphere Servers.

It is strongly recommended that you add a vCenter Server or ESX(i) hosts to the backup infrastructure before you add the storage system. When you add the storage system, Veeam Backup & Replication performs the storage system rescan. As a part of this process, Veeam Backup & Replication maps storage volumes to VMware vSphere datastores. This helps Veeam Backup & Replication understand what VMs host their disks on storage volumes.

If you add the storage system to the backup infrastructure and do not add the vCenter Server or ESX(i) hosts, you will be able to perform only restore from storage snapshots. You will not be able to perform Backup from Storage Snapshots.

**TIP:**

If you first add the storage system to the backup infrastructure and then add the vCenter Server or ESX(i) host, perform storage rescan to map storage volumes to VMware vSphere datastores.
Configuring Backup Proxy

For some operations with storage snapshots, Veeam Backup & Replication requires a backup proxy. The backup proxy is used for two purposes:

- Rescan of VMFS on storage volumes
- Backup from Storage Snapshot

When Veeam Backup & Replication performs rescan and backup operations, it needs to read the content on storage volumes and snapshots. To do this, Veeam Backup & Replication uses a backup proxy as a helper. Storage volumes and snapshots are mounted as new volumes to the backup proxy. As a result, Veeam Backup & Replication can access mounted volumes and snapshots over the backup proxy and read VM data from them.

To enable storage rescan and Backup from Storage Snapshots, you must configure a backup proxy in the backup infrastructure. The backup proxy must meet the requirements listed below.

General Requirements

- The role of a backup proxy must be assigned to a Microsoft Windows machine. This can be a dedicated machine or backup server performing the role of the default backup proxy.
- For Backup from Storage Snapshots, the transport mode for the backup proxy must be set to Automatic selection or Direct storage access.
- [For HPE 3PAR] If storage LUNs reside in a virtual domain, the backup proxy to which LUNs are exported must reside in the same virtual domain. If LUNs reside outside a virtual domain, the backup proxy must also reside outside any available virtual domain.

iSCSI Protocol

- The backup proxy must have a Microsoft iSCSI Software initiator enabled.
- iSCSI traffic between the backup proxy and storage system must be allowed.

**NOTE:**

For storage rescan, Veeam Backup & Replication uses its own initiator. For this reason, a Microsoft iSCSI Software initiator may not be enabled when you perform storage rescan. For Backup from Storage Snapshots, however, a Microsoft iSCSI Software initiator must be enabled.

Fibre Channel Protocol

- The backup proxy must have a Fibre channel adapter installed and must have access to the storage system over Fibre Channel fabric.
- To let Veeam Backup & Replication present snapshots of LUNs to the backup proxy, you must register the backup proxy with a WWN ID on the storage system.
- Fibre Channel devices must be properly installed and shown in Device Manager on the backup proxy. The WWN ID of the backup proxy must be properly zoned on the Fibre Channel switch.
NFS Protocol

NFS traffic between the backup proxy and storage system must be allowed.
Enabling HPE 3PAR Web Services API Server

This step must be performed if you plan to work with the HPE 3PAR StoreServ storage system.

Veeam Backup & Replication uses the HPE 3PAR Web Services API server to communicate with the HPE 3PAR StoreServ storage system. When you add the HPE 3PAR StoreServ storage to the backup infrastructure, Veeam Backup & Replication attempts to enable the server automatically. If Veeam Backup & Replication fails to enable the server automatically, for example, Veeam Backup & Replication does not have enough privileges to do this, you need to enable the server manually.

**IMPORTANT!**

The HPE 3PAR Web Services API is a part of the HPE 3PAR OS starting from version 3.1.2. Veeam Backup & Replication does not support earlier versions of the HPE 3PAR OS.

To check if the HPE 3PAR Web Services API server is enabled and enable it if needed:

1. Log on to the Processor with administrator privileges:

   ```
   #ssh <administrator account>@<SP IP Address>
   ```

2. View the current state of the Web Services API Server:

   ```
   #showwsapi
   ```

   ```
   -- -State- -HTTP_State- HTTP_Port -HTTPS_State- HTTPS_Port -Version-
   Enabled Active Enabled       8008
   Enabled       8080         1.1
   ```

3. If the Web Services API Server is disabled, start it:

   ```
   #startwsapi
   ```

4. If the HTTP or HTTPS state is disabled, enable one of them:

   ```
   #setwsapi -http enable
   ```

   or

   ```
   #setwsapi -https enable
   ```
Adding Storage Systems

To use storage snapshots for data protection and disaster recovery operations, you must add the storage system to the backup infrastructure. If you plan to work with secondary storage arrays, you must add them to the backup infrastructure as well.

When you add the storage system, Veeam Backup & Replication automatically rescans it. As part of the rescan process, Veeam Backup & Replication performs the following operations:

1. Veeam Backup & Replication retrieves information about the storage system topology.
2. Veeam Backup & Replication retrieves information about VMware vSphere datastores from the vCenter Server and matches storage volumes to these datastores. Matching helps Veeam Backup & Replication understand what VMs host their disks on storage volumes. It also helps Veeam Backup & Replication get information about VMs on storage snapshots. Veeam Backup & Replication assumes that disks of VMs located on storage volumes are also located on storage snapshots.
3. Veeam Backup & Replication rescans storage snapshots. As a result of snapshot rescan, Veeam Backup & Replication knows exactly what disks of what VMs are hosted on storage snapshots. If for some reason Veeam Backup & Replication fails to rescan all storage snapshots, it rescans the last storage snapshot in the hierarchy and propagates the retrieved information to other storage snapshots.

The topology of the storage system added to the backup infrastructure is displayed in the Storage Infrastructure view in the Veeam Backup & Replication console. Storage snapshots are also displayed in the inventory pane of the Home view, under the Storage snapshots node.

You can add the following storage systems to the backup infrastructure:

- Dell EMC
- IBM Spectrum Virtualize
- Universal Storage API Integrated Systems
- HPE StoreVirtual
- HPE 3PAR StoreServ
- HPE Nimble
- NetApp Data ONTAP
- Cisco HyperFlex

Adding Dell EMC VNX, VNXe/Unity

Before you add a storage system to the backup infrastructure, check prerequisites. Then use the New DELL EMC Storage wizard to add the storage system.

1. Launch the New Dell EMC Storage wizard
2. Select the storage type
3. Specify the storage name or address
4. Specify credentials
5. Specify access options
6. Finish working with the wizard
Step 1. Launch New Dell EMC Storage Wizard

To launch the New Dell EMC Storage wizard, do one of the following:

- Open the Storage Infrastructure view. In the working area, click Add Storage. In the displayed window, click DELL EMC.
- Open the Storage Infrastructure view. In the inventory pane, right-click the Storage Infrastructure node and select Add Storage. In the displayed window, click DELL EMC.
- You can use this method if at least one Dell EMC storage system is added to the backup infrastructure. Open the Storage Infrastructure view. In the inventory pane, right-click the DELL EMC node and select Add storage. You can also select the DELL EMC node in the inventory pane, right-click anywhere in the working area and select Add storage.

Add Storage
Select vendor of the primary storage systems your virtual machines reside on. You can see and manage all registered storage systems on the Storage Infrastructure tab.

- Cisco HyperFlex
  Adds Cisco HyperFlex systems (H3C Series/SpringPath).
- Dell EMC
  Adds Dell EMC VNX, VNX2, VNXe and Unity storage. Fibre Channel (FC), iSCSI and NFS connectivity is supported.
- Hewlett Packard Enterprise
  Adds HPE 3PAR StoreServ, HPE StoreVirtual or HPE Nimble Storage.
- IBM Spectrum Virtualize
  Adds IBM SAN Volume Controller (SVC), IBM Storwize and systems based on IBM Spectrum Virtualize software, including Lenovo Storage and IBM/Cisco VersaStack.
- NetApp
  Adds NetApp ONTAP or NetApp SolidFire storage.

Get plug-in for another storage...
Opens a Veeam web page where you can browse available plug-ins and download the one from your storage vendor.

Step 2. Select Storage Type

At the Storage Type step of the wizard, select the storage type.

- Select VNX (block) to add a Dell EMC VNX block storage system working over iSCSI or Fibre Channel.
- Select VNX (file) to add a Dell EMC VNX file storage system working over NFS.
- Select VNXe to add a Dell EMC VNXe storage system.
• Select **Unity** to add a Dell EMC Unity storage system.

### Step 3. Specify Storage Name or Address

At the **Name** step of the wizard, specify the storage system name and description.

1. In the **DNS name or IP address** field, specify a DNS name or IP address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

---

![New Dell EMC Storage dialog box](image)

- **Name**: Storage system by providing IP address or DNS name of storage processor (SP) for VNX Block, or management interface for VNXe, VNX File and Unity.
- **Storage Type**: DNS name or IP address
- **Description**: Dell EMC VNXe Storage System

---

**Step 4. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see Managing Credentials.

2. **[For Dell EMC VNX block storage]** Select the scope to which the user account belongs:
   - Select **Global** if the user can administrate all VNX systems in the domain.
   - Select **Local** if the user can administrate only a single VNX storage system in the domain.
   - Select **LDAP** if the user can administrate all VNX systems that use the LDAP server for authentication.

3. When you add a storage system, Veeam Backup & Replication saves to the configuration database the following information:
   - **[For Dell EMC VNXe/Unity]** A thumbprint of the TLS certificate installed on the management server.
   - **[For Dell EMC VNX file storage]** A fingerprint of the SSH key of the management server.

During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid man-in-the-middle attacks.
[For Dell EMC VNXe/Unity] If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click View.
- If you trust the server, click Continue.
- If you do not trust the server, click Cancel.

Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

[For Dell EMC VNX file storage] To let you identify the server, Veeam Backup & Replication displays the SSH key fingerprint. To accept the fingerprint and connect to the server, click Yes. If you click No, Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

If you update the certificate or SSH key on the server, you must acknowledge the new certificate or SSH key in the server connection settings. To do this, in the Storage Infrastructure view right-click the storage system, select Edit storage, pass through the Edit Server wizard and click Trust.

Step 5. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.
To select volumes for rescan:

a. On the right of the **Volumes to scan** field, click **Choose**.

b. In the **Choose Volumes** window, select volumes that you want to rescan. To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list. To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

   If you leave the **Automatic detection** option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see [Rescanning Storage Systems](#).

3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   o Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

   o Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.
NOTE:

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the Failover to standard backup option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.
Step 6. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

Adding IBM Spectrum Virtualize

Before you add a storage system to the backup infrastructure, check prerequisites. Then use the **New IBM Spectrum Virtualize Storage** wizard.

1. **Launch the New IBM Spectrum Virtualize Storage wizard**
2. **Specify the storage name or address**
3. **Specify credentials**
4. **Specify access options**
5. **Finish working with the wizard**

Before You Begin

Before you add a storage system to the backup infrastructure, make sure that a license for the IBM Spectrum Virtualize storage system supports IBM FlashCopy.
Step 1. Launch New IBM Spectrum Virtualize Storage Wizard

To launch the New IBM Spectrum Virtualize Storage wizard, do one of the following:

- Open the Storage Infrastructure view. In the working area, click Add Storage. In the displayed window, click IBM Spectrum Virtualize.
- Open the Storage Infrastructure view. In the inventory pane, right-click the Storage Infrastructure node and select Add Storage. In the displayed window, click IBM Spectrum Virtualize.
- You can use this method if at least one IBM Spectrum Virtualize storage system is added to the backup infrastructure.

Open the Storage Infrastructure view. In the inventory pane, right-click the IBM Spectrum Virtualize node under Storage Infrastructure and select Add storage. You can also select the IBM Spectrum Virtualize node in the inventory pane, right-click anywhere in the working area and select Add storage.

Step 2. Specify Storage Name or Address

At the Name step of the wizard, specify the storage system name and description.

1. In the DNS Name or IP address field, specify a DNS name or IP address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

![New IBM Spectrum Virtualize Storage](image)

**Step 3. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the Credentials list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right of the Credentials field to add the credentials. For more information, see Managing Credentials.

**NOTE:**

User name and password values are case-sensitive.
2. The default port for communication with the storage system is 22. If necessary, you can change the port number in storage system settings and specify the new port number in the Port field.

Step 4. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

To select volumes for rescan:

   a. On the right of the Volumes to scan field, click Choose.

   b. In the Choose Volumes window, select volumes that you want to rescan. To exclude volumes from rescan, select All volumes except, click Add and select volumes from the list. To rescan only specific volumes, select Only these volumes, click Add and select volumes from the list.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

IMPORTANT!

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.
3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

- Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

- Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

**NOTE:**

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see **Configuring Backup from Storage Snapshots**.

![New IBM Spectrum Virtualize Storage](image)
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

![New IBM Spectrum Virtualize Storage Wizard](image)

Adding Universal Storage API Integrated Systems

Before you add a Universal Storage API integrated system to the backup infrastructure, check prerequisites. Then use the storage installation wizard.

1. **Launch the storage installation wizard**
2. **Specify the storage name or address**
3. **Specify credentials**
4. **Specify access options**
5. **Finish working with the wizard**

Step 1. Launch Storage Installation Wizard

To launch a storage installation wizard for Universal Storage API integrated systems, perform the following steps.

1. Open the **Storage Infrastructure** view and do one of the following:
   - In the working area, click **Add Storage**.
   - In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**.
2. In the displayed window, click **Show more vendors** and select the storage system that you want to add. To launch the installation wizard for NetApp SolidFire storage systems, in the displayed window select **NetApp > Element**.

You can use this method to launch the wizard if at least one Universal Storage API integrated system is added to the backup infrastructure:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, right-click the necessary storage system and select **Add Storage**. Alternatively, you can select the necessary storage system in the inventory pane, right-click anywhere in the working area and select **Add storage**.

---

**Add Storage**

Select vendor of the primary storage system your virtual machines reside on. You can see and manage all registered storage systems on the **Storage Infrastructure** tab.

- **Huawei**
  - Adds Huawei OceanStor Series storage devices. Fibre Channel (FC), iSCSI and NFS connectivity is supported.

- **INFINIDAT InfiniBox**
  - Adds InfiniBox F-series systems. Fibre Channel (FC), iSCSI and NFS connectivity is supported.

- **Pure Storage**
  - Adds Pure Storage FlashArray. FC and iSCSI connectivity is supported.

- **Get plug-in for another storage...**
  - Opens a Veeam web page where you can browse available plugins, and download the one from your storage vendor.

---

**Step 2. Specify Storage Name or Address**

At the **Name** step of the wizard, specify the storage system name and description.

1. In the **DNS Name or IP address** field, specify a DNS name or IP address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

![New INFINIDAT InfiniBox Storage](image)

**Step 3. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the Credentials list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the Manage accounts link or click Add on the right of the Credentials field to add the credentials. For more information, see Managing Credentials.

**NOTE:**

User name and password values are case-sensitive.
2. The default port for communication with the storage system is 443. If necessary, you can change the port number in storage system settings and specify the new port number in the Port field.

Step 4. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes for rescan:
   
   a. On the right of the Volumes to scan field, click Choose.

   b. In the Choose Volumes window, select volumes that you want to rescan. To exclude volumes from rescan, select All volumes except, click Add and select volumes from the list. To rescan only specific volumes, select Only these volumes, click Add and select volumes from the list.

   If you leave the Automatic detection option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

IMPORTANT!

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.
3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the Backup proxies to use field, click Choose and define backup proxies that you want to use for these operations.

   - Select Automatic selection to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.
   
   - Select Use the selected backup proxy servers only to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

**NOTE:**

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the Failover to standard backup option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

![Summary screenshot](image)

### Adding HPE StoreVirtual

To add an HPE StoreVirtual storage system to the backup infrastructure, use the **New HPE StoreVirtual Storage** wizard.

1. **Launch the New HPE StoreVirtual Storage wizard**
2. **Specify the storage name or address**
3. **Specify credentials**
4. **Specify access options**
5. **Finish working with the wizard**

**Step 1. Launch New HPE StoreVirtual Storage Wizard**

To launch the **New HPE StoreVirtual Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **StoreVirtual**.

- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **StoreVirtual**.
You can use this method if at least one HPE StoreVirtual storage system is added to the backup infrastructure.

Open the Storage Infrastructure view. In the inventory pane, right-click the HPE StoreVirtual node under Storage Infrastructure and select Add storage. You can also select the HPE StoreVirtual node in the inventory pane, right-click anywhere in the working area and select Add storage.

**Step 2. Specify Storage Name or Address**

At the **Name** step of the wizard, specify the storage system name and description.

1. On the right of the **Management server DNS name or IP address** field, click **Browse** and select an HPE storage management group.
   
   You can also type a DNS name or IP address of the storage management server or storage cluster in the **Management server DNS name or IP address** field.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the management group, date and time when the HPE management group was added.

**Step 3. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the management group.

1. From the **Credentials** list, select credentials to connect to the management group. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see Managing Credentials.

**NOTE:**

User name and password values are case-sensitive.

2. When you add a storage system, Veeam Backup & Replication saves a fingerprint of the SSH key of the management server to the configuration database. During every subsequent connection to the server, Veeam Backup & Replication uses the saved fingerprint to verify the server identity and avoid man-in-the-middle attacks.

To let you identify the server, Veeam Backup & Replication displays the SSH key fingerprint.

- If you trust the server and want to connect to it, click **Yes**.
- If you do not trust the server, click **No**. Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.
If you update the SSH key on the server, you must acknowledge the new key in the server connection settings. To do this, in the Storage Infrastructure view right-click the storage system, select Edit storage, pass through the Edit Server wizard and click Trust to acknowledge the new key.

![New HPE StoreVirtual Storage](image)

### Step 4. Specify Access Options

At the **Access Options** step of the wizard, specify options for accessing the storage system.

1. The **Protocol to use** list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes for rescan:
   
   a. On the right of the **Volumes to scan** field, click **Choose**.

   b. In the **Choose Volumes** window, select volumes that you want to rescan. To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list. To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

   If you leave the **Automatic detection** option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see **Rescanning Storage Systems**.
IMPORTANT!

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the Backup proxies to use field, click Choose and define backup proxies that you want to use for these operations.

- Select Automatic selection to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

- Select Use the selected backup proxy servers only to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

NOTE:

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the Failover to standard backup option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.
Step 5. Finish Working with Wizard

At the Summary step of the wizard, review settings of the added storage system and click Finish to start the rescan process.

Adding HPE 3PAR StoreServ

Before you add an HPE 3PAR StoreServ storage system to the backup infrastructure, check prerequisites. Then use the New HPE 3PAR StoreServ Storage wizard to add the storage system.

1. Launch the New HPE 3PAR StoreServ Storage wizard
2. Specify the HPE 3PAR Web Services API address
3. Specify credentials
4. Specify access options
5. Finish working with the wizard

Before You Begin

Before you add a storage system to the backup infrastructure, check the following prerequisites:

1. The HPE 3PAR Web Services API server must be enabled. For more information, see Enabling HPE 3PAR Web Services API Server.
2. A license for the HPE 3PAR StoreServ storage system must support HPE 3PAR Virtual Copy.
Step 1. Launch New HPE 3PAR StoreServ Storage Wizard

To launch the **New HPE 3PAR StoreServ Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **3PAR StoreServ**.

- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **3PAR StoreServ**.

- You can use this method if at least one HPE 3PAR StoreServ storage system is added to the backup infrastructure.

Open the **Storage Infrastructure** view. In the inventory pane, right-click the **HPE 3PAR StoreServ** node under **Storage Infrastructure** and select **Add storage**. You can also select the **HPE 3PAR StoreServ** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.

---

Step 2. Specify HPE 3PAR Web Services API Address

Veeam Backup & Replication uses the HPE 3PAR Web Services API to work with HPE 3PAR StoreServ storage systems. The HPE 3PAR Web Services API delivers a programming interface for performing storage management tasks.

At the **Name** step of the wizard, provide information about the HPE 3PAR Web Services API Server.

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the HPE 3PAR Web Services API Server.
2. In the **URL** field, enter a URL of the HPE 3PAR Web Services API Server. By default, Veeam Backup & Replication uses the following URL:

   `https://<websapiserver>:8080`

   where `<websapiserver>` is the name or IP address of the HPE 3PAR Web Services API Server.

3. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the server, date and time when the server was added.

   ![New HPE 3PAR StoreServ Storage](image)

   **Name:** Register HPE 3PAR StoreServ by specifying DNS name or IP address of the storage.

   **Credentials**

   **Access Options**

   **Summary**

   DNS name or IP address:
   
   hp3
   
   URL:
   
   `https://hp3:8080`
   
   Description:
   
   HPE StoreServ Storage

   **Step 3. Specify Credentials**

   At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the HPE 3PAR Web Services API Server.

   1. From the **Credentials** list, select credentials to connect to the HPE 3PAR Web Services API Server. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the necessary credentials. For more information, see Managing Credentials.

   **IMPORTANT!**

   The user account must have the ‘edit’ user role on the HPE 3PAR Web Services API Server.

   2. When you add a storage system, Veeam Backup & Replication saves to the configuration database a TLS certificate thumbprint and an SSH key fingerprint of the HPE 3PAR Web Services API Server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid the man-in-the-middle attack.
If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click View.
- If you do not trust the server, click Cancel.
  Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.
- If you trust the server, click Continue.
  Veeam Backup & Replication will display the SSH key fingerprint. To accept the fingerprint and connect to the server, click Yes.

If you update the certificate or SSH key on the server, you must acknowledge the new certificate or SSH key in the server connection settings. To do this, in the Storage Infrastructure view right-click the storage system, select Edit storage, pass through the Edit Server wizard and click Trust.

Step 4. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.
To select volumes for rescan:

a. On the right of the Volumes to scan field, click Choose.

b. In the Choose Volumes window, select volumes that you want to rescan. To exclude volumes from rescan, select All volumes except, click Add and select volumes from the list. To rescan only specific volumes, select Only these volumes, click Add and select volumes from the list.

If you leave the Automatic detection option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.

IMPORTANT!

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the Backup proxies to use field, click Choose and define backup proxies that you want to use for these operations.

   o Select Automatic selection to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

   o Select Use the selected backup proxy servers only to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.
NOTE:

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see Configuring Backup from Storage Snapshots.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

![New HPE 3PAR StoreServ Storage](image)

Adding HPE Nimble

To add an HPE Nimble storage system to the backup infrastructure, use the **New HPE Nimble Storage** wizard.

1. **Launch the New HPE Nimble Storage wizard**
2. **Specify the storage name or address**
3. **Specify credentials**
4. **Specify access options**
5. **Finish working with the wizard**

Step 1. Launch New Nimble Storage Wizard

To launch the **New HPE Nimble Storage** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **Nimble**.

- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Hewlett Packard Enterprise** and select **Nimble**.

- You can use this method if at least one HPE Nimble storage system is added to the backup infrastructure.
Open the **Storage Infrastructure** view. In the inventory pane, right-click the **HPE Nimble** node under **Storage Infrastructure** and select **Add Storage**. You can also select the **HPE Nimble** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.

**Add HPE Storage**
Select your Hewlett Packard Enterprise storage model.

- **3PAR StoreServ**
  Adds HPE 3PAR StoreServ storage. Fibre Channel (FC) and iSCSI connectivity is supported.

- **Nimble**
  Adds HPE Nimble AF-Series, HP-Series and CS-Series storage. Fibre Channel (FC) and iSCSI connectivity is supported.

- **StoreVirtual**
  Adds HPE StoreVirtual (LeftHand/P4000) and HPE StoreVirtual VSA (Virtual Storage Appliance) storage. Only iSCSI connectivity is supported.

**Step 2. Specify Storage Name or Address**

At the **Name** step of the wizard, specify the storage system name and description.

1. In the **DNS name or IP address** field, specify a DNS name or IP address of the storage system.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

### New HPE Nimble Storage

<table>
<thead>
<tr>
<th>Name</th>
<th>DNS name or IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[172.16.21.43]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Nimble Storage</td>
</tr>
</tbody>
</table>

**Step 3. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see Managing Credentials.

   The user account that you select must have Administrator or Power User permissions on the HPE Nimble storage system.

2. Veeam Backup & Replication uses HPE Nimble RESTful API to communicate with the storage system. By default, commands to the RESTful API server are sent over port 5392. If you use another port for HPE Nimble RESTful API, you can change the port number.

3. When you add a storage system, Veeam Backup & Replication saves to the configuration database the following information:
   - [For Nimble OS 2.3 and later] A thumbprint of the TLS certificate installed on the management server.
   - [For Nimble OS 2.3] A fingerprint of the SSH key of the management server.

   During every subsequent connection to the server, Veeam Backup & Replication uses the saved information to verify the server identity and avoid man-in-the-middle attacks.
[For Nimble OS 2.3 and later] If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click View.
- If you trust the server, click Continue.
- If you do not trust the server, click Cancel.

Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

[For Nimble OS 2.3] To let you identify the server, Veeam Backup & Replication displays the SSH key fingerprint. To accept the fingerprint and connect to the server, click Yes. If you click No, Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.

If you update the certificate or SSH key on the server, you must acknowledge the new certificate or SSH key in the server connection settings. To do this, in the Storage Infrastructure view, right-click the storage system, select Edit storage, pass through the Edit Server wizard and click Trust.

Step 4. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.
To select volumes for rescan:

a. On the right of the **Volumes to scan** field, click **Choose**.

b. In the **Choose Volumes** window, select volumes that you want to rescan. To exclude volumes from rescan, select **All volumes except**, click **Add** and select volumes from the list. To rescan only specific volumes, select **Only these volumes**, click **Add** and select volumes from the list.

If you leave the **Automatic detection** option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see [Rescanning Storage Systems](#).

**IMPORTANT!**

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

3. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.
NOTE:

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected in the job settings is not added to the list of backup proxies in the storage system connection settings, Veeam Backup & Replication will fail over to the regular data processing mode. For more information, see Configuring Backup from Storage Snapshots.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

![New HPE Nimble Storage Summary](image_url)

---

**Adding NetApp Data ONTAP**

Before you add to the backup infrastructure a NetApp storage system running Data ONTAP, check prerequisites. Then use the **New NetApp Data ONTAP Storage** wizard to add the storage system.

1. Launch the New NetApp Data ONTAP Storage wizard
2. Specify the NetApp server name or address
3. Specify credentials and protocol type
4. Specify access options
5. Rescan the storage system

**Step 1. Launch New NetApp Data ONTAP Storage Wizard**

To launch the **New NetApp Data ONTAP Storage** wizard, perform the following steps.

1. Open the **Storage Infrastructure** view and do one of the following:
   - In the working area, click **Add Storage**.
   - In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**.
2. In the displayed window, select **NetApp > Data ONTAP**.
You can use this method to launch the wizard if at least one NetApp storage system is added to the backup infrastructure:

1. Open the **Storage Infrastructure** view.
2. In the inventory pane, right-click the necessary NetApp storage system and select **Add Storage**. Alternatively, you can select the necessary NetApp storage system in the inventory pane, right-click anywhere in the working area and select **Add storage**.

Step 2. Specify NetApp Server Name or Address

At the **Name** step of the wizard, specify the storage system name and description.

1. In the **Management server DNS name or IP address** field, specify a DNS name or IP address of the storage system.

   You can browse for storage systems that exist in your environment:
   
   a. On the right of the **Management server DNS name or IP address** field, click **Browse**.
   
   b. In the **NetApp Storage System Discovery** window, enter an IP address of the storage system or IP address of the subnet where the storage is located and click **Discover**. Veeam Backup & Replication will search the whole subnet for storage systems. For example, if you enter 172.16.1.12 as an IP address, Veeam Backup & Replication will search storage systems in subnet 172.16.1.* and display a list of storage systems detected in this subnet.
   
   c. In the list below, select a storage system that you want to add.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the storage system was added.

---

### Step 3. Specify Credentials and Protocol Type

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system, and select the transport protocol.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see Managing Credentials.

2. From the **Protocol** list, select the type of protocol over which you want to communicate with the storage system: **HTTP** or **HTTPS**.

   The default transport protocol is HTTPS. However, you can configure the storage system to communicate with Veeam Backup & Replication over the HTTP protocol if needed.
3. The default port for communication with the storage system is 443. If necessary, you can change the port number in storage system settings and specify the new port number in the Port field.

4. When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the NetApp management server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

- To view detailed information about the certificate, click View.
- If you trust the server, click Continue.
- If you do not trust the server, click Cancel.

Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.
If you update the certificate on the server, you must acknowledge the new certificate in the server connection settings. To do this, in the Storage Infrastructure view right-click the storage system, select Edit storage, pass through the Edit Server wizard and click Trust to acknowledge the new certificate.

Step 4. Specify Access Options

At the Access Options step of the wizard, specify options for accessing the storage system.

1. The Protocol to use list displays protocols over which the storage system can work. Select check boxes next to protocols over which you want to work with the storage system.

2. [For NetApp storage system working over NFS] During storage rescan, backup and restore operations, Veeam Backup & Replication automatically creates required NFS export rules on the storage system. If you do not want Veeam Backup & Replication to create export rules, clear the Create required NFS export rules automatically check box.

3. If you plan to work with specific storage volumes, you can limit the storage rescan scope. In this case, Veeam Backup & Replication will rescan only the volumes that you select. Limiting the rescan scope reduces the amount of time required for the rescan operation.

   To select volumes for rescan:
   a. On the right of the Volumes to scan field, click Choose.
   b. In the Choose Volumes window, select volumes that you want to rescan. To exclude volumes from rescan, select All volumes except, click Add and select volumes from the list. To rescan only specific volumes, select Only these volumes, click Add and select volumes from the list.

   If you leave the Automatic detection option selected, Veeam Backup & Replication will rescan all volumes in the storage hierarchy.

After you finish working with the wizard, you can change the rescan scope and start the rescan process manually at any time. For more information, see Rescanning Storage Systems.
IMPORTANT!

If you plan to use Backup from Storage Snapshots, you need to make sure that you include in the rescan scope volumes on which VM disks reside.

4. Operations of storage rescan and Backup from Storage Snapshots are performed with the help of a backup proxy. On the right of the **Backup proxies to use** field, click **Choose** and define backup proxies that you want to use for these operations.

   - Select **Automatic selection** to let Veeam Backup & Replication pick a backup proxy automatically. Veeam Backup & Replication will check which backup proxies have access to the storage system, and automatically assign an optimal backup proxy for rescan and Backup from Storage Snapshots.

   - Select **Use the selected backup proxy servers only** to explicitly select a backup proxy that must be used for rescan and Backup from Storage Snapshots. It is recommended that you select at least two backup proxies to ensure that rescan and Backup from Storage Snapshot are performed if one of backup proxies fails or loses its connectivity to the storage system.

**NOTE:**

If you select backup proxies explicitly, you must make sure that you also select these proxies in settings of backup and replication jobs for which you plan to use Backup from Storage Snapshots. If a backup proxy selected for the job is not added to the list of backup proxies in the storage system connection settings and the **Failover to standard backup** option is disabled in the job settings, the job will fail. For more information, see [Configuring Backup from Storage Snapshots](#).
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

Adding Cisco HyperFlex

Before you add a Cisco HyperFlex storage system to the backup infrastructure, **check prerequisites**. Then use the **New Cisco HyperFlex System** wizard to add the storage system.

1. **Launch New Cisco HyperFlex System wizard**
2. **Specify the storage name or address**
3. **Specify credentials**
4. **Specify a backup proxy**
5. **Finish working with the wizard**

Step 1. Launch New Cisco HyperFlex System Wizard

To launch the **New Cisco HyperFlex System** wizard, do one of the following:

- Open the **Storage Infrastructure** view. In the working area, click **Add Storage**. In the displayed window, click **Cisco HyperFlex**.
- Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Storage Infrastructure** node and select **Add Storage**. In the displayed window, click **Cisco HyperFlex**.
- You can use this method if at least one Cisco HyperFlex storage system is added to the backup infrastructure.
Open the **Storage Infrastructure** view. In the inventory pane, right-click the **Cisco HyperFlex** node under **Storage Infrastructure** and select **Add Storage**. You can also select the **Cisco HyperFlex** node in the inventory pane, right-click anywhere in the working area and select **Add storage**.

---

**Add Storage**

Select vendor of the primary storage system your virtual machines reside on. You can see and manage all registered storage systems on the Storage Infrastructure tab.

- **Cisco HyperFlex**
  Adds Cisco HyperFlex systems (HX Series/OpeningPath).

- **Dell EMC**
  Adds Dell EMC VNX, VMAX, VPLEX and Unity storage. Fibre Channel (FC), iSCSI and NFS connectivity is supported.

- **Hewlett Packard Enterprise**
  Adds HPE 3PAR StoreServ, HPE StoreVirtual or HPE Nimble storage.

- **IBM Spectrum Virtualize**
  Adds IBM SAN Volume Controller (SVC), IBM StorWize and systems based on IBM Spectrum Virtualize software, including Lenovo Storage and IBM/Cisco VersaStack.

- **NetApp**
  Adds NetApp ONTAP or NetApp SolidFire storage.

- **Get plug-in for another storage**
  Opens a Veeam web page where you can browse available plug-ins, and download the one from your storage vendor.

---

**Step 2. Specify Storage Name or Address**

At the **Name** step of the wizard, specify the storage system name and description.

1. In the **DNS name or IP address** field, enter a full DNS name or IP address of the Cisco HyperFlex cluster management interface.
2. In the **Description** field, provide a description for future reference. The default description contains information about the user who added the storage system, date and time when the server was added.

![New Cisco HyperFlex System](image)

**Step 3. Specify Credentials**

At the **Credentials** step of the wizard, specify credentials for a user account with administrator privileges on the storage system.

1. From the **Credentials** list, select credentials to connect to the storage system. If you have not set up credentials beforehand, click the **Manage accounts** link or click **Add** on the right of the **Credentials** field to add the credentials. For more information, see Managing Credentials.

2. When you add a storage system, Veeam Backup & Replication saves to the configuration database a thumbprint of the TLS certificate installed on the Cisco HyperFlex RESTful API server. During every subsequent connection to the server, Veeam Backup & Replication uses the saved thumbprint to verify the server identity and avoid the man-in-the-middle attack.

   If the certificate installed on the server is not trusted, Veeam Backup & Replication displays a warning.

   - To view detailed information about the certificate, click **View**.
   - If you trust the server, click **Continue**.
   - If you do not trust the server, click **Cancel**.

     Veeam Backup & Replication will display an error message, and you will not be able to connect to the server.
If you update the certificate on the server, you must acknowledge the new certificate in the server connection settings. To do this, in the **Storage Infrastructure** view right-click the storage system, select **Edit storage**, pass through the **Edit Server** wizard and click **Trust** to acknowledge the new certificate.

**Step 4. Specify Backup Proxy**

At the **Access Options** step of the wizard, click **Choose** and select backup proxies that you plan to use for backup and replication of VMs hosted on Cisco HyperFlex. Veeam Backup & Replication will check what data retrieval methods are available for these backup proxies. For more information, see **Methods of Data Retrieval**.

- Select **Automatic selection** to let Veeam Backup & Replication check data retrieval methods for all backup proxies in the backup infrastructure.
- Select **Use the selected backup proxy servers only** to explicitly define backup proxies that will be used for VM data processing. In this case, Veeam Backup & Replication will check data retrieval methods only for selected backup proxies.
Step 5. Finish Working with Wizard

At the **Summary** step of the wizard, review settings of the added storage system and click **Finish** to start the rescan process.

After you click **Finish**, we will modify firewall rules on system `cisco-hyperflextech.local`. You can view the progress by opening the corresponding session log.
Rescanning Storage Systems

You can rescan a storage system added to the backup infrastructure. Storage system rescan may be required, for example, if you create or delete snapshots on the storage system. Storage system rescan will help you discover these changes and update the storage system hierarchy in the Veeam Backup & Replication console.

Storage system rescan can be performed automatically or manually.

- **Automatic storage rescan**: Veeam Backup & Replication uses the following processes to rescan the storage system:
  - The *Storage Monitor* process runs in the background. The process detects new snapshots and volumes, and performs their rescan with a time interval of 10 minutes.
  - The *Storage Discovery* process starts every 7 days. The process performs rescan of the whole storage system or selected volumes (if you limited the rescan scope for the storage system).

- **Manual storage rescan**: if necessary, you can start the *Storage Discovery* process manually. Storage discovery can be performed against any node in the storage system hierarchy: storage system, storage volume and so on.

Before you start storage discovery, make sure that you have a properly configured backup proxy in the backup infrastructure. Otherwise, Veeam Backup & Replication will not be able to match storage volumes to VMware datastores and locate VMs on these storage volumes.

**NOTE:**
Veeam Backup & Replication does not perform rescan on VMs whose disks are located on VVol datastores.

To start storage discovery:

1. Open the *Storage Infrastructure* view.
2. In the inventory pane, expand the storage system tree.
3. Select a node in the storage system hierarchy: storage system, volume and so on.
4. Click *Rescan* on the ribbon or right-click the node in the hierarchy and select *Rescan storage* or *Rescan volume.*
IMPORTANT!

The rescan operation is performed only for volumes included in the rescan scope. To change the rescan scope, open the storage system connection settings and navigate to the Access Options step of the wizard. For details, see Adding Storage System.

Limiting Rescan Scope

The storage system hierarchy can be very extensive, and the rescan process can take much time. To minimize the rescan time, you can instruct Veeam Backup & Replication to rescan only specific volumes.

To limit the rescan scope:

1. Open the Storage Infrastructure view.
2. In the inventory pane, select the storage system type.
3. In the working area, right-click the root node of the storage system and click Choose volumes.
4. In the Choose Volumes window, select which volumes you want to rescan:
   - To exclude volumes from rescan, select All volumes except, click Add and select volumes in the list.
   - To rescan only specific volumes, select Only these volumes, click Add and select volumes in the list.

   If you leave the Automatic detection option selected, Veeam Backup & Replication will rescan all volumes in the storage system hierarchy.
5. Click OK.
6. Click Finish.
Removing Storage Systems

You can remove a storage system from the backup infrastructure, for example, if you do not want to perform Backup from Storage Snapshots or use Veeam Explorer from Storage Snapshots anymore.

Mind the following:

- When you remove a storage system from the backup infrastructure, Veeam Backup & Replication attempts to find hosts with IQN starting with the ‘VeeamAUX’ prefix and remove such objects from the storage hierarchy. Veeam Backup & Replication assumes that such hosts are created by Veeam Backup & Replication itself and are used for service purposes.

- You cannot remove a storage system from the backup infrastructure if you have a snapshot job configured for this storage system. You must delete the snapshot job first.

To remove a storage system:

1. Open the Storage Infrastructure view.

2. In the inventory pane or in the working area, right-click the storage system and select Remove storage.
Backup from Storage Snapshots

Backup from Storage Snapshots lets you speed up backup and replication for VMware vSphere VMs whose disks are hosted on storage systems. When you perform Backup from Storage Snapshots, Veeam Backup & Replication leverages storage snapshots for VM data processing. Backup from Storage Snapshots lets you reduce impact of backup and replication activities on the production environment and improve RPOs.
VM Data Processing

Backup from Storage Snapshots introduces a different mode of data processing for VMware vSphere VMs whose disks are hosted on storage systems.

Regular VM Data Processing

In the regular processing course, Veeam Backup & Replication uses a VMware vSphere snapshot. The VMware vSphere snapshot “freezes” the VM state and data at a specific point in time. This way, the VM data is brought to a consistent state suitable for backup or replication.

During regular VM data processing, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication triggers a VMware vSphere snapshot for a VM. VM disks are put to the read-only state, and every virtual disk of the VM receives a delta file named like `vmname-00001.vmdk`.

2. Veeam Backup & Replication copies VM data from read-only disks of the VM. All changes that the user makes to the VM while backup or replication is performed are written to delta files.

3. When VM processing is finished, the VMware vSphere snapshot is committed. VM disks resume writes, and data from delta files is merged to the VM disks. After data is merged, the VMware vSphere snapshot is removed.

Regular VM data processing may take long. If backup or replication is performed for a VM running a highly transactional application, the delta file may grow large. The snapshot commit process will take much time, and the VM may hang up during this process. To overcome this situation, you can use Backup from Storage Snapshots.

Backup from Storage Snapshots

Backup from Storage Snapshots lets you speed up backup and replication operations. For Backup from Storage Snapshots, Veeam Backup & Replication complements the VMware vSphere snapshot technology with the storage snapshots technology, and uses storage snapshots as a source of data for backup and replication.

During Backup from Storage Snapshots, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication triggers a VMware vSphere snapshot for VMs whose disks are hosted on the storage system.

2. Veeam Backup & Replication triggers a storage snapshot of the volume or LUN hosting the VM itself and the created VMware vSphere snapshot.

3. The VMware vSphere snapshot on the original storage volume is deleted immediately after the storage snapshot is created. Veeam Backup & Replication accesses the ‘cloned’ VMware vSphere snapshot on the storage snapshot and copies VM data from it.

4. When VM processing is finished, the storage snapshot capturing the VMware vSphere snapshot is removed.
As a result, the VMware vSphere snapshot exists for a very short time, namely several seconds. Delta files do not grow large, and the time of VMware vSphere snapshot commit decreases.
Backup from Primary Storage Arrays

To use Backup from Storage Snapshots, you must select the **Enable backup from storage snapshots** check box in backup or replication job settings.

When you run a job with Backup from Storage Snapshots enabled, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication analyzes which VMs in the job host their disks on the storage system, and triggers the vCenter Server to create VMware vSphere snapshots for these VMs.
2. Veeam Backup & Replication gets Changed Block Tracking information for VMs hosted on the storage system.
3. Veeam Backup & Replication instructs the storage system to create a snapshot of the storage volume or LUN that hosts VM disks and VMware vSphere snapshots.
4. Veeam Backup & Replication instructs the vCenter Server to remove VMware vSphere snapshots on the production storage system. The 'cloned' VMware vSphere snapshots remain on the created storage snapshots.
5. Veeam Backup & Replication checks the backup infrastructure and detects if there is a backup proxy that has a direct connection to the storage system. Veeam Backup & Replication mounts the storage snapshot as a new volume to this backup proxy.
6. Veeam Backup & Replication reads and transports VM data blocks via the backup proxy to the backup repository. For incremental backup or replication, Veeam Backup & Replication uses obtained CBT data to retrieve only changed data blocks from the storage snapshot.
7. When VM data processing is finished, Veeam Backup & Replication unmounts the storage snapshot from the backup proxy and instructs the storage system to remove the storage snapshot.

Mixed Job Scenarios

Backup from Storage Snapshots is used only for those VMs whose disks are hosted on supported storage systems. As backup and replication jobs typically process a number of VMs that may reside on different types of storage, Veeam Backup & Replication processes VMs in mixed jobs in the following way:

- If a job processes a number of VMs whose disks are hosted on different types of storage, Veeam Backup & Replication uses Backup from Storage Snapshots only for VMs whose disks are hosted on supported storage systems. Other VMs are processed in a regular manner.
- If a VM has several disks, some hosted on supported storage systems and some hosted on another type of storage, Veeam Backup & Replication does not use Backup from Storage Snapshots to such VM. All disks of such VM are processed in a regular manner.

During a job, Veeam Backup & Replication processes VMs residing on different types of storage at different time:

1. Veeam Backup & Replication first triggers VMware vSphere snapshots and storage snapshots for VMs hosted on supported storage systems.
2. After the storage snapshot is created, Veeam Backup & Replication triggers VMware vSphere snapshots for other VMs. These VMs are processed in a regular manner further on, in parallel with VMs whose disks are hosted on supported storage systems.

Configuring Backup from Storage Snapshots

You can instruct Veeam Backup & Replication to use Backup from Storage Snapshots for backup and replication. During backup and replication jobs, Veeam Backup & Replication reads data of processed VMs from storage snapshots, which speeds up backup and replication operations and improves RPOs.

Before you perform Backup from Storage Snapshots, check the following prerequisites:

- You must configure the backup infrastructure in a proper way:
  - You must add to the backup infrastructure a backup proxy that will be used for backup or replication, and properly configure this backup proxy. For more information, see Configuring Backup Proxy.
You must add to the backup infrastructure vCenter Server or ESX(i) hosts with VMs whose disks are hosted on the storage system.

You must add the storage system to the backup infrastructure.

- You must check limitations for Backup from Storage Snapshots. For more information, see Backup from Storage Snapshots.

To back up and replicate VMs using Backup from Storage Snapshots:

1. Configure a backup or replication job. At the Storage step of the backup or replication job wizard, select a backup proxy that will be used for data transport. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

NOTE:
A backup proxy that you select must be added to the list of backup proxies in storage system connection settings. If the backup proxy is not added to the list in storage system connection settings, Veeam Backup & Replication will fail over to the regular data processing mode. For more information, see Adding Storage Systems.

2. At the Storage step of the wizard, click Advanced, then click the Integration tab. Make sure that the Enable backup from storage snapshots check box is selected. By default, this option is enabled for all newly created jobs.

3. If you add to the job many VMs whose disks are hosted on the same volume or LUN, select the Limit processed VM count per storage snapshot to <N> check box and specify the number of VMs for which 1 storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate storage snapshot for every VM group. As a result, the job performance will increase. For more information, see Limitation on Number of VMs per Snapshot.
4. If Veeam Backup & Replication fails to create a storage snapshot, VMs whose disks are hosted on the storage system will not be processed by the job. To fail over to the regular data processing mode and back up or replicate such VMs, select the **Failover to standard backup** check box.
Backup from Secondary Storage Arrays

If the primary storage array is associated with a secondary storage array, you can use the secondary storage array as a data source for backup. Backup from snapshots on secondary storage arrays reduces impact on the production storage. During backup, operations on VM data reading are performed on the side of the secondary storage array, and the primary storage array is not affected.

You can use backup from snapshots on secondary storage arrays if you have the following storage systems in the production environment:

- HPE 3PAR Peer Persistence
- IBM Spectrum Virtualize with HyperSwap function
- HPE Nimble arrays with replicated copies
- NetApp SnapMirror and/or NetApp SnapVault

To back up from snapshots on secondary storage arrays, you must configure the backup job to build a snapshot chain on the secondary storage array and instruct Veeam Backup & Replication to use the created snapshots as a data source.

How Backup from Secondary Storage Systems Works

Backup from snapshots on secondary storage arrays is similar to Backup from Storage Snapshots on the primary storage array.

1. Veeam Backup & Replication triggers a VMware vSphere snapshot for a VM whose disks are hosted on the primary storage array.
2. Veeam Backup & Replication instructs the storage system to create an application-consistent storage snapshot on the primary storage array. The created snapshots capture the VMware vSphere snapshot. The VMware vSphere snapshot on the primary storage array is then deleted.

3. The storage snapshot is transported from the primary storage array to the secondary storage array.

4. Veeam Backup & Replication checks if there is a backup proxy that has a direct connection to the secondary storage array. The transported storage snapshot is mounted to this backup proxy.

5. The backup job retrieves VM data from the mounted storage snapshot.

6. When the job finishes processing the VM, Veeam Backup & Replication instructs the storage system to delete a snapshot on the primary storage array. The transported snapshot on the secondary storage remains in the snapshot chain until it is removed by the retention policy.

Mind the following:

- [For HPE Nimble] On HPE Nimble storage systems, snapshot transport is triggered as soon as you create a new storage snapshot. For this reason, launch of snapshot transport and deletion of VMware vSphere snapshots are performed in parallel.

- [For NetApp] Veeam Backup & Replication creates auxiliary snapshots on the primary storage system. The number of storage snapshots in the snapshot chain cannot be fewer than 1.

---

**Failover to Backup from Snapshots on Primary Storage Arrays**

In some cases, Veeam Backup & Replication may fail to back up VM data from storage snapshots on the secondary storage array. This can happen, for example, if Veeam Backup & Replication fails to connect to the secondary storage array or a license required for volume or LUN export is not installed (in case of NetApp SnapMirror or SnapVault).

To overcome this situation, you can instruct the backup job to fail over to the Backup from Storage Snapshots on the primary storage array. In this case, Veeam Backup & Replication will create a storage snapshot on the primary storage array and attempt to transport it to the secondary storage array. If the transport process fails, Veeam Backup & Replication will retrieve VM data from the created snapshot on the primary storage array.

To let Veeam Backup & Replication fail over to Backup from Storage Snapshots on the primary storage array, you must enable the **Failover to primary storage snapshot option** in the backup job settings.
NOTE:
Failover to Backup from Storage Snapshots on the primary storage array is not supported for HPE 3PAR Peer Persistence and IBM Spectrum Virtualize with HyperSwap function.

Configuring Backup from Snapshots on Secondary Storage Arrays
You can configure a backup job to perform Backup from Storage Snapshots on secondary storage arrays.
Before you run the backup job, check the following prerequisites:

- You must configure a secondary storage array for the primary storage system where VMs that you plan to back up are hosted.
- You must install a license for Veeam Backup & Replication Enterprise Plus edition on the backup server.
- You must configure the backup infrastructure in a proper way:
  - [For HPE Nimble] You must configure Volume Collection replication from the primary storage array to the secondary storage array. For more information, see HPE Nimble documentation.
  - [For NetApp] You must configure volume SnapMirror/Snapvault relationships between the primary and secondary storage arrays. For more information, see NetApp documentation.
  - You must add to the backup infrastructure a backup proxy that will be used for backup, and properly configure this backup proxy. For more information, see Configuring Backup Proxy.
  - You must add to the backup infrastructure vCenter Server or ESX(i) hosts with VMs whose disks are hosted on the storage system.
You must add the primary storage system and secondary storage array to the backup infrastructure.

[For IBM Spectrum Virtualize with HyperSwap function] You must add IBM Spectrum Virtualize storage system to the backup infrastructure, and select secondary storage volumes as a data source for backup using registry keys. For more information, contact Veeam Customer Support.

IMPORTANT!

When you add storage arrays to the backup infrastructure, you must add to the rescan scope volumes and LUNs on which VM disks are located (both for primary and secondary storage arrays). For more information, see Adding Storage Systems.

- You must check limitations for Backup from Storage Snapshots. For more information, see Backup from Storage Snapshots.
- [For NetApp] You must install a license for storage snapshot export on NetApp SnapMirror or SnapVault. For more information, see Required Licenses for NetApp.

To back up VMs from snapshots on secondary storage arrays:

1. Configure a backup job. At the Storage step of the backup job wizard, select a backup proxy that will be used for data transport. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

NOTE:

A backup proxy that you select must be added to the list of backup proxies in storage system connection settings. If the backup proxy is not added to the list in storage system connection settings, Veeam Backup & Replication will fail over to the regular data processing mode. For more information, see Adding Storage Systems.
2. From the **Backup repository** list, select a backup repository where you want to store backup files.

3. In the **Retention policy** section, specify the number of backup restore points that you want to keep.

4. Select the **Configure secondary destinations for this job** check box.

5. Click **Advanced**, then click the **Integration** tab. Make sure that the **Enable backup from storage snapshots** check box is selected. By default, this option is enabled for all newly created jobs.

6. If you add to the job many VMs whose disks are located on the same volume or LUN, select the **Limit processed VM count per storage snapshot to <N>** check box and specify the number of VMs for which 1 storage snapshot must be created. Veeam Backup & Replication will divide VMs into several groups and trigger a separate storage snapshot for every VM group. As a result, the job performance will increase. For more information, see [Limitation on Number of VMs per Snapshot](#).

7. If Veeam Backup & Replication fails to create a storage snapshot, VMs whose disks are located on the storage system will not be processed by the job. To fail over to the regular data processing mode and back up such VMs, select the **Failover to standard backup** check box.
8. If Veeam Backup & Replication cannot create a storage snapshot on the secondary storage array, the job will not back up VMs whose disks are located to the storage system. To fail over to Backup from Storage Snapshots on the primary storage system, select the **Failover to primary storage snapshot** check box. If Veeam Backup & Replication fails to create a storage snapshot on the secondary storage array, it will trigger the storage snapshot on the primary storage system and use it as a source for backup. Note, however, that Backup from Storage Snapshots on the primary storage system will produce additional load on the production environment.

![Advanced Settings dialog box](image)

9. At the **Secondary Target** step of the wizard, click **Add** and select a secondary storage array. For example, **Nimble Snapshot Replicated Copy**.

10. In the **Number of snapshot copies to retain** field, specify the number of storage snapshots that you want to maintain in the snapshot chain on the secondary storage array. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain.

    This option is not applicable to NetApp SnapMirror and HPE 3PAR StoreServ Peer Persistence. On these secondary storage systems, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage arrays.
11. Select the **Use as the data source** check box.

12. Specify other backup job settings as required.

13. Click **Next**, then click **Finish** to save the job settings.
Limitation on Number of VMs per Snapshot

By default, during Backup from Storage Snapshots Veeam Backup & Replication creates VMware vSphere snapshots for all VMs that reside on the same volume or LUN, and then triggers a storage snapshot for this volume or LUN. If the number of VMs on the volume or LUN is great, VM snapshot creation may take much time. To speed up the backup or replication process, you can limit the number of VMs per storage snapshot.

To limit the number of storage snapshots, you must enable the Limit processed VM count per storage snapshot to <N> option and specify the number of VMs per snapshot in the job settings.

With the limitation option enabled, Veeam Backup & Replication processes VMs in several cycles:

1. Veeam Backup & Replication divides VMs into several groups, as defined in the Limit processed VM count per storage snapshot to <N> option.
2. Veeam Backup & Replication triggers VMware vSphere snapshots for VMs in the first group.
3. Veeam Backup & Replication triggers a storage snapshot for the volume or LUN on which VMs are hosted.
4. Veeam Backup & Replication deletes VMware vSphere snapshots for VMs in the first group.
5. Veeam Backup & Replication copies data of VMs in the first group from the storage snapshot.
6. Veeam Backup & Replication removes the storage snapshot.
7. Steps 2-6 are repeated for every remaining group of VMs.

For example, you add to the job 15 VMs whose disks are hosted on the same volume and set the Limit processed VM count per storage snapshot to <N> option to 10. Veeam Backup & Replication will divide all VMs into 2 groups — a group of 10 VMs and group of 5 VMs. Veeam Backup & Replication will perform the data processing cycle for the first group of VMs. When VM data processing is over, Veeam Backup & Replication will start processing the second group of VMs.
Backup from Cisco HyperFlex Snapshots

Veeam Backup & Replication integrates with Cisco HyperFlex and allows you to improve performance of backup and replication of VMware vSphere VMs hosted on Cisco HyperFlex.

For backup and replication of VMs hosted on Cisco HyperFlex, Veeam Backup & Replication does not use VMware vSphere snapshots to preserve VMs in a consistent state suitable for backup or replication. Instead, it relies on native Cisco HyperFlex VM snapshots. Use of Cisco HyperFlex VM snapshots lets avoid the overhead produced by VMware vSphere snapshots removal on the production environment.

To create HyperFlex VM snapshots, Cisco leverages VMware vSphere Storage APIs Array Integration (VAAI). VAAI enables VMware vSphere ESX(i) hosts to communicate with storage devices and offload storage operations such as snapshot creation and cloning to the storage array. As a result, Cisco HyperFlex can create space efficient VM snapshots almost instantly. Veeam Backup & Replication, in its turn, can use HyperFlex snapshots for VM data processing, which helps speed up backup and replication operations, reduce impact of backup and replication activities on the production environment and improve RPOs.

Implementation of integration with Cisco HyperFlex is different from those provided for other supported storage systems. When Veeam Backup & Replication processes VMs hosted on Cisco HyperFlex, it leverages snapshots created at the VM level, not snapshots created at the storage volumes level. The results of the VM processing are reported in job results: if a VM is processed with Cisco HyperFlex snapshots, Veeam Backup & Replication displays the ‘Creating VM native Cisco HX snapshot’ message in job statistics.
Integration Modes

Veeam Backup & Replication provides two types of integration for Cisco HyperFlex:

- **Advanced integration with Cisco HyperFlex**
- **Standard data processing with Direct NFS enhancements**

Advanced Integration with Cisco HyperFlex

In case of full integration with Cisco HyperFlex, Veeam Backup & Replication can leverage Cisco HyperFlex VM snapshots for backup and replication, which improves VM data processing performance.

Veeam Backup & Replication fully integrates with Cisco HyperFlex if the production environment and backup infrastructure meet the following requirements:

- VMs reside on the supported Cisco HyperFlex system. For more information, see System Requirements.
- Veeam Backup & Replication 9.5 Update 2 or later is installed on the backup server.
- License for Veeam Backup & Replication Enterprise Plus Edition is installed on the backup server.
- Cisco HyperFlex system is added to the backup infrastructure. For more information, see Adding Cisco HyperFlex Storage System.
- Backup proxy is properly configured in the backup infrastructure. For more information, see Configuring Backup Proxies.
- The Enable backup from storage snapshots option is selected in the job settings (default setting). For more information, see Configuring Backup of VMs on Cisco HyperFlex.

You can instruct Veeam Backup & Replication to read data from Cisco HyperFlex snapshots in the following transport modes: Direct storage access, Virtual appliance or Network. The recommended mode is Direct storage access working over NFS protocol. It provides the best performance and low overhead on ESX(i) hosts. In this mode, Veeam Backup & Replication bypasses the ESX(i) host and reads/writes data directly from/to Cisco HyperFlex NFS data network.

Standard Data Processing with Direct NFS Enhancements

Veeam Backup & Replication can use standard backup methods to process VMs hosted on Cisco HyperFlex. In this case, Veeam Backup & Replication will leverage standard VMware vSphere VM snapshots, not Cisco HyperFlex VM snapshots to preserve VMs in a consistent state suitable for backup or replication.

To allow Veeam Backup & Replication to access VM data directly over the HyperFlex Data network by NFS protocol, Veeam has added some enhancements starting from Veeam Backup & Replication v9.0 Update 2. Veeam Backup & Replication can use the Direct NFS access transport mode if the production environment and backup infrastructure meet the following requirements:

- Direct NFS access is enabled on data platform controllers. For more information, [https://www.veeam.com/kb2300](https://www.veeam.com/kb2300).
- VMs do not have Cisco HyperFlex snapshots (including the base snapshot) or VMware vSphere snapshots.
- VMs meet requirements described in the Limitations for Direct NFS access section.
- Backup proxies assigned for jobs work in the Direct storage access or Automatic selection modes. For more information, see Adding VMware Backup Proxies.
• Backup data read over NFS is processed by a single HyperFlex Controller that holds the HyperFlex Controller Cluster IP.

If these requirements are not met, Veeam Backup & Replication can process VM data in the Virtual appliance or Network transport mode.

The diagram below demonstrates how Veeam Backup & Replication picks transport modes for processing VMs hosted on Cisco HyperFlex:
How Backup from Cisco HyperFlex Snapshots Works

When you perform backup or replication from Cisco HyperFlex snapshots, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication analyses which VMs in the job are hosted on Cisco HyperFlex.
2. If application-aware processing is enabled, Veeam Backup & Replication quiesces data and applications on VMs guest OSes.
3. Veeam Backup & Replication triggers Cisco HyperFlex VM snapshots through VAAI individually for every processed VM.
4. If application-aware processing is enabled, Veeam Backup & Replication resumes quiesced I/O activities on VMs guest OSes.
5. Veeam Backup & Replication reads new virtual disk data blocks (for full job session) or changed virtual disk data blocks with CBT (for incremental job sessions) from Cisco HyperFlex NFS stores and transports them to the backup repository or target datastore.
6. After VM data processing is finished, Veeam Backup & Replication triggers removal of the Cisco HyperFlex VM snapshots.

**NOTE:**
After the backup job completes, the HyperFlex Sentinel snapshot (base snapshot) remains for the VM and is visible in the VMware Snapshot Manager. This is done to improve the processing performance and reduce storage load. For more information, see the Cisco HyperFlex documentation.
Configuring Backup Proxies

To enable backup and replication from Cisco HyperFlex snapshots, you must configure one or more backup proxies in the backup infrastructure. Backup proxies must meet the following requirements:

- The role of a backup proxy must be assigned to a Microsoft Windows machine. This can be a dedicated machine or backup server performing the role of the default backup proxy.
- The backup proxy that you plan to use must have NFS access to the network handling traffic between Cisco HyperFlex and ESXi hosts where the backed-up or replicated VMs reside.

Methods of Data Retrieving

Backup proxies that process data of VMs hosted on Cisco HyperFlex can read VM data from NFS stores over the NFS HyperFlex data network. Depending on the backup infrastructure configuration, backup proxies can read data over the following data paths:

- **Backup from Storage Snapshots over IO Visor on ESXi(i) hosts.** The IO Visor is a Cisco HyperFlex software module that runs on every ESXi host that is a part of the Cisco HyperFlex cluster. It presents HyperFlex NFS datastores to the ESXi(i) hosts and optimizes the data paths in the HyperFlex cluster.
  
  The backup over IO Visor is the preferred method. It provides the high speed of VM data reading and balances the load across the HyperFlex cluster. To read VM data over IO Visor, backup proxies must be connected to the same HyperFlex data network as the processed VMs. You must also configure a firewall rule on the ESXi hosts to allow Veeam Backup & Replication to interact with the IO Visor. For more information, see Configuring Firewall Rules for Cisco HyperFlex IO Visor Processing.

  If the firewall rules are not configured, Veeam Backup & Replication will fail over to Backup from Storage Snapshot over the HyperFlex Controller Cluster IP by default.

- **Backup from Storage Snapshots over HyperFlex Controller Cluster IP.** In this processing mode, all traffic is handled by a single HX controller that holds the HyperFlex Controller Cluster IP.
  
  To read VM data over HyperFlex Controller Cluster IP, backup proxies must be connected to the same HyperFlex data network as the processed VMs. Veeam Backup & Replication will configure all necessary firewall settings within the HyperFlex Controllers automatically during the storage discovery process. Veeam Backup & Replication automatically detects new HyperFlex controllers and applies firewall changes.

Configuring Firewall Rules for Cisco HyperFlex IO Visor Processing

The Cisco HyperFlex IO Visor is a software component that runs on all ESXi hosts within a Cisco HyperFlex cluster. It works as a NFS server for Veeam traffic.

You need to allow NFS traffic from the backup proxies to ESXi hosts. As Cisco IO Visor based NFS communication uses dynamic ports, you need to create an ESXi firewall rule with inbound ports 0-65535 and the backup proxy IP addresses as allowed IP addresses.

You can do this in 3 ways:

- Create a VMware ESXi host extension VIB file that creates the firewall rule, install/enable it on all hosts and set the backup proxy IP addresses as allowed ones. For more information, see https://www.veeam.com/kb2291.
- Use a predefined VMware ESXi host extension VIB file from the Veeam Community GitHub project. For more information, see https://www.veeam.com/kb2298.
• Use ESXi command line interface to create a temporary firewall rule (until the next ESXi host reboot). For more information, see https://www.veeam.com/kb2299.

Configuring Backup Proxies for Backup from Storage Snapshot with Virtual Appliance or Network mode

If you plan to use the Virtual appliance or Network mode to process VMs hosted on Cisco HyperFlex, you must configure the backup infrastructure in the following way:

1. You must add Cisco HyperFlex to the backup infrastructure to allow Veeam Backup & Replication to create HyperFlex snapshots.

2. You must configure the backup proxies to work in the Virtual appliance or Network transport mode. For more information, see Virtual Appliance and Network Mode.

3. If you plan to use the Virtual appliance mode, it is recommended that you enable an optimization for NFS datastores in Veeam Backup & Replication to avoid VM stuns as described in http://kb.vmware.com/kb/2010953. To do this:
   a. Create a backup proxy on every host in the VMware vSphere cluster where VMs that you plan to back up or replicate reside.
   b. On the machine where the Veeam Backup & Replication console is installed, open Registry Editor.
   c. Navigate to the key: HKLM\Software\Veeam\Veeam Backup and Replication\.
   d. Create a new DWORD with name EnableSameHostHotaddMode, and set its value to 2. If a backup proxy on the same host as a processed VM is unavailable, Veeam Backup & Replication will use an available backup proxy on a different host, but force it to use the Network transport mode, so that no stun occurs.
Configuring Backup from Cisco HyperFlex Snapshots

You can instruct Veeam Backup & Replication to perform backup and replication from Cisco HyperFlex snapshots. During a backup and replication job, Veeam Backup & Replication will use native Cisco HyperFlex VM snapshots instead of VMware vSphere snapshots, which will speed up backup and replication operations and improve RPOs.

Before you configure backup and replication jobs, make sure that the production environment and backup infrastructure meet requirements for full integration with Cisco HyperFlex. For more information, see Integration Modes.

To back up and replicate from Cisco HyperFlex snapshots:

1. Configure a backup or replication job. At the Storage step of the backup or replication job wizard, select a backup proxy that will be used for data transport. You can assign the backup proxy explicitly or choose the automatic mode of backup proxy selection.

2. At the Storage step of the wizard, click Advanced, then click the Integration tab. Make sure that the Enable backup from storage snapshots check box is selected. By default, this option is enabled for all newly created jobs.
3. If Veeam Backup & Replication fails to process VMs in the full integration mode, VMs hosted on Cisco HyperFlex will not be backed up or replicated. To fail over to the regular data processing mode, select the **Failover to standard backup** check box.
Configuring Direct NFS Access on Cisco HyperFlex (Earlier Than 2.0)

VMware vSphere VMs hosted on Cisco HyperFlex access the storage with the help of special Cisco HyperFlex HX Data Platform controllers. The controllers are dedicated VMs deployed on the same VMware ESX host that hosts the VMs.

By default, the controllers are configured to receive traffic only from the ESX(i) host where they are located. To provide communication between Veeam Backup & Replication and the Cisco HyperFlex storage system, you need to manually enable the Direct NFS access mode between the backup proxy and controllers.

For more information about configuring Direct NFS Access on Cisco HyperFlex earlier than 2.0, see https://www.veeam.com/kb2300.
Snapshot Orchestration

Veeam Backup & Replication lets you perform Snapshot Orchestration — build a snapshot chain on primary and/or secondary storage arrays. To create snapshots on storage arrays, you must run a snapshot-only job.

The snapshot-only job is similar to scheduling automatic snapshot creation in the storage management console. A snapshot-only job does not create Veeam backup files on the backup repository. It creates only storage snapshots on the storage system by a schedule that is defined in the job settings.

Depending on the backup job settings, the created snapshots can be application-consistent or crash-consistent.
Configuring Snapshot-Only Jobs

You can use snapshot-only jobs to create a chain of storage snapshots on the primary storage array and, optionally, on the secondary storage array.

To configure a snapshot-only job:

1. Open the Home view.
2. Click Backup Job > VMware or vCloud on the ribbon. Veeam Backup & Replication will launch the New Backup Job wizard.
3. At the Name step of the wizard, specify a name and description for the backup job.
4. At the Virtual Machines step of the wizard, click Add and select VMs whose disks are hosted on the storage system.
5. At the Storage step of the wizard, select the primary storage array from the Backup repository list.
6. In the Restore points to keep on disk field, specify the number of storage snapshots that you want to maintain in the snapshot chain on the primary storage array. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the snapshot chain.

Mind that the number of snapshots in the snapshot chain on the primary storage array cannot be fewer than 1. Even if you set the Restore points to keep on disk value to 0, Veeam Backup & Replication will keep 1 snapshot in the snapshot chain.

7. If you want to additionally create storage snapshots on the secondary storage array, select the Configure secondary destinations for this job check box.

8. If you have enabled a secondary destination for the job, at the Secondary Target step of the wizard, click Add and select the secondary storage array for a secondary location.
9. [For secondary storage arrays] In the **Number of snapshot copies to retain** field, specify the number of storage snapshots that you want to maintain in the snapshot chain on the secondary storage array. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the chain.

**NOTE:**

The **Number of snapshot copies to retain** option is not applicable to NetApp SnapMirror and HPE 3PAR Peer Persistence. On these secondary storage systems, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage systems.

If you use SnapMirror relationships between QTrees, you can define different retention policy settings for the primary NetApp storage system and NetApp SnapMirror. For example, you can configure the backup job to maintain 14 snapshots on the primary NetApp storage system and 10 snapshots of QTree directories on NetApp SnapMirror.
10. To create application-consistent storage snapshots, you can enable VMware Tools quiescence or application-aware processing. If you do not enable either of these options, Veeam Backup & Replication will produce a crash-consistent storage snapshot.

   - To enable VMware Tools quiescence, in the advanced settings of the backup job select the **Enable VMware Tools quiescence** check box. Veeam Backup & Replication will use VMware Tools to create VMware vSphere snapshots for VMs whose disks are hosted on the storage system. After VMware vSphere snapshots are created, Veeam Backup & Replication will trigger a storage snapshot. For more information, see VMware Tools Quiescence.

   - To enable application-aware processing, at the **Guest Processing** step of the wizard select the **Enable application-aware processing** check box and specify necessary settings for application-aware image processing.
During the backup job session, Veeam Backup & Replication will quiesce applications running inside VMs using application-aware processing. After applications inside the VM are quiesced, Veeam Backup & Replication will trigger a storage snapshot. For more information, see Application-Aware Processing.

11. At the Schedule step of the wizard, select the Run the job automatically check box and specify the schedule by which storage snapshots must be created. For more information, see Define Job Schedule. For more information, see Define Job Schedule in Veeam Backup & Replication User Guide for VMware vSphere.

12. Click Next, then click Finish to save the backup job settings.
Backup from Storage Snapshots with Snapshot Retention

You can configure a backup job to create regular backup files on the backup repository and, additionally, maintain a snapshot chain on the storage system. Veeam Backup & Replication lets you create storage snapshots in the following destinations:

- Primary storage array where VM disks are hosted
- Secondary storage arrays

Depending on the backup job settings, the created storage snapshots can be application-consistent or crash-consistent.

The backup job of this type is performed in the following way:

1. Veeam Backup & Replication triggers the vCenter Server to create a VMware vSphere snapshot for a VM.
2. Veeam Backup & Replication instructs the storage system to create two snapshots of a volume or LUN capturing VM disks:
   - A new snapshot on the storage system. This snapshot remains in the snapshot chain until it is removed by the retention policy.
   - A temporary snapshot for backup or replication operations. This snapshot is removed after backup or replication is complete.
3. Veeam Backup & Replication removes the created VMware vSphere snapshot from the VM snapshot list.
4. Veeam Backup & Replication uses the temporary storage snapshot as a data source for backup and replication.
5. Veeam Backup & Replication performs cleanup operations and removes the temporary snapshot on the storage array.
6. Veeam Backup & Replication checks the number of storage snapshots in the snapshot chain. If the number exceeds the value defined in retention policy settings, Veeam Backup & Replication instructs the storage system to remove the earliest snapshot from the snapshot chain.
## Configuring Backup Jobs with Storage Snapshot Retention

You can configure a backup job to create backup files and a chain of storage snapshots on the primary storage array and/or secondary storage arrays.

Before you perform backup, configure the backup infrastructure in a proper way:

- **[For HPE Nimble]** You must configure Volume Collection replication from the primary storage array to the secondary storage array. For more information, see HPE Nimble documentation.
- **[For NetApp]** You must configure volume SnapMirror/Snapvault relationships between the primary and secondary storage arrays. For more information, see NetApp documentation.

To configure a backup job:

1. Open the **Home** view.
2. Click **Backup Job > VMware** or vCloud on the ribbon. Veeam Backup & Replication will launch the **New Backup Job** wizard.
3. At the **Name** step of the wizard, specify a name and description for the backup job.
4. At the **Virtual Machines** step of the wizard, select VMs whose disks are hosted on the storage system.
5. At the **Storage** step of the wizard, from the **Backup repository** list select a backup repository where you want to store backup files.
6. In the **Retention policy** section, specify the number of backup restore points that you want to keep.
7. Select the **Configure secondary destinations for this job** check box.
8. At the **Secondary Target** step of the wizard, click **Add** and select primary or secondary storage arrays to create snapshots.

9. In the **Number of snapshot copies to retain** field, specify the number of storage snapshots that you want to maintain in the snapshot chain. When this number is exceeded, Veeam Backup & Replication will trigger the storage system to remove the earliest snapshot from the snapshot chain. Mind that the number of snapshots in the snapshot chain on the primary storage array cannot be fewer than 1.

**NOTE:**

The **Number of snapshot copies to retain** option is not applicable to NetApp SnapMirror and HPE 3PAR Peer Persistence. On these secondary storage systems, Veeam Backup & Replication maintains the same number of storage snapshots as on primary storage systems.

If you use SnapMirror relationships between QTrees, you can define different retention policy settings for the primary NetApp storage system and NetApp SnapMirror. For example, you can configure the backup job to maintain 14 snapshots on the primary NetApp storage system and 10 snapshots of QTree directories on NetApp SnapMirror.

10. Specify other backup job settings as required.

11. Click **Next**, then click **Finish** to save the job settings.
Veeam Explorer for Storage Snapshots

Veeam Explorer for Storage Snapshots is a technology in Veeam Backup & Replication that lets you restore VMware VM data directly from native storage snapshots. Veeam Explorer for Storage Snapshots automates the process of data recovery for VMs hosted on storage systems, eliminates intermediate restore and manual operations. As a result, you can restore necessary VM data from storage snapshots in seconds.

You can use Veeam Explorer for Storage Snapshots to perform the following restore operations:

- Instant VM Recovery
- VM guest OS files restore (Microsoft Windows and multi-OS restore)
- Restore of Microsoft Active Directory objects
- Restore of Microsoft Exchange objects
- Restore of Microsoft SharePoint objects
- Restore of Microsoft SQL Server databases
- Restore of Oracle databases
Traditional Restore vs. Restore from Storage Snapshots

Many organizations use storage snapshots for data protection. Storage snapshots allow for very low RPO: they have minimal impact on storage performance and can be created in seconds. Administrators can schedule snapshots to be created several times a day or even every hour.

In virtual environments, restore from storage snapshots can be difficult. Storage snapshots are created per-volume, and a volume typically hosts disks of several VMs. For this reason, restore from storage snapshots is not a simple rollback operation — it is a multi-task process. If restore from storage snapshots is performed manually, an administrator must do the following:

1. Present a storage snapshot to an ESX(i) host.
2. Perform an HBA rescan.
3. Mount the storage snapshot to an ESX(i) host.
4. Browse the storage snapshot to locate VM files.
5. Add the VM to the inventory or copy VM files to another VMFS datastore.
6. Power on the VM.
7. Perform restore operations.
8. Perform cleanup operations after VM data restore is complete.

As a result, the restore process takes much time. If you need to restore guest OS files and application objects from a VM on the storage snapshot, the procedure will be even more complicated.

Veeam Explorer for Storage Snapshots fully automates operations of mounting storage snapshots to ESX(i) hosts. You only need to select an ESX(i) host to which the storage snapshot will be mounted, and Veeam Explorer for Storage Snapshots will perform all other operations automatically.

Veeam Explorer for Storage Snapshots does not convert storage snapshots into backups. It uses them as is and lets you restore VM data directly from native storage system snapshots. You do not have to install any agents or perform additional configuration actions.
How Restore from Storage Snapshots Works

For restore operations, Veeam Backup & Replication uses a copy of the volume snapshot, not the volume snapshot itself.

The volume snapshot copy is a read-write clone of the volume snapshot. The volume snapshot copy protects the VMFS volume metadata integrity on the volume snapshot. During file-level restore and Instant VM Recovery, the ESX(i) host to which the volume snapshot is mounted updates VMFS metadata on the volume snapshot. Use of the volume snapshot copy helps protect the volume snapshot from these changes.

When you restore VM data from storage snapshots, Veeam Backup & Replication performs the following actions:

1. The user starts the restore process for a VM on the storage snapshot.
2. Veeam Backup & Replication triggers the storage system to create a copy or a clone of this storage snapshot.
   - If you restore several VMs from one storage snapshot, Veeam Backup & Replication does not create several snapshot copies. Instead, it uses one snapshot copy for restore.
   - If you start several restore operations (for example, Instant VM Recovery and VM guest OS restore) for the same VM from the storage snapshot, Veeam Backup & Replication creates several snapshot copies and works with them during restore.
3. The user selects an ESX(i) host in the virtual environment, and the created snapshot copy is presented to this ESX(i) host as a new volume. The ESX(i) host is added to the list of Allowed Servers for the snapshot copy. As a result, the ESX(i) host has access to the snapshot copy and can read and write data to/from it.
4. Veeam Backup & Replication makes sure that the IP address of the storage system is in the list of static targets on the ESX(i) host.
5. The storage system issues an HBA rescan command to the vCenter Server. Once rescan is finished, the snapshot copy appears in the discovered targets list on the ESX(i) host. After that, the storage system performs re-signature for storage volumes.
6. The user performs necessary restore operations in the Veeam Backup & Replication console.
7. After restore is completed, Veeam Backup & Replication issues a command to the storage system. The storage system deletes the snapshot copy from the ESX(i) host and performs cleanup operations.
Creating and Deleting Snapshots

You can create and delete storage snapshots in the Veeam Backup & Replication console. The create/delete snapshot operations do not differ from operations that you perform in the management console of the storage system.

To create a volume snapshot:

1. Open the Storage Infrastructure view.
2. In the inventory pane, expand the storage system tree.
3. Right-click the necessary volume and select Create Snapshot.
4. In the New Storage Snapshot window, specify a name for the created snapshot and provide a description for the snapshot (if the snapshot description field is available).
5. [For HPE StoreVirtual] To quiesce VMs on the volume, select the Create application-managed snapshot check box. The storage system will trigger a command to the vCenter Server to quiesce VMs with VMware Tools. VM quiescence will bring VM data to a consistent state before the snapshot is taken. If the Create application-managed snapshot option is not enabled, Veeam Backup & Replication will trigger a point-in-time snapshot.

NOTE:

To create application-managed snapshots on HPE StoreVirtual, make sure that Application Aware Snapshot Manager is properly installed and configured. If the Application Aware Snapshot Manager is not installed, Veeam Backup & Replication will report an error, and the snapshot will not be created. For more information, see HPE StoreVirtual Application-Aware Snapshot Manager Deployment Guide.
To delete a volume snapshot:

1. Open the Storage Infrastructure view.
2. In the inventory pane, expand the storage system tree.
3. Right-click the necessary snapshot and select Delete snapshot.
Performing Instant VM Recovery

You can instantly recover a VM from a storage snapshot without prior de-staging and intermediate restores. Instant VM Recovery accelerates VM restore, improves RTOs and decreases downtime of production VMs.

Before performing Instant VM Recovery, check prerequisites. Then use the Instant Recovery wizard to restore a VM from a storage snapshot.

1. Launch the Instant Recovery wizard
2. Select a VM
3. Select a restore point
4. Select a recovery mode
5. Select a destination for the recovered VM
6. Specify a restore reason
7. Verify Instant VM Recovery settings
8. Finalize Instant VM Recovery

Before You Begin

Before you perform Instant VM Recovery, check the following prerequisites:

- If you are recovering a VM to the production network, make sure that the original VM is powered off to avoid conflicts.
- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch Instant Recovery Wizard

To launch the Instant Recovery wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere backup. In the Restore from backup section, select Instant VM recovery.
- Open the Storage Infrastructure view. In the inventory pane, expand the storage system tree and select the necessary volume snapshot. In the working area, select a VM that you want to restore and click Instant VM Recovery on the ribbon. You can also right-click a VM and select Instant VM recovery. In this case, you will pass immediately to the Recovery Mode step of the wizard.
- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM that you want to restore and click Instant VM Recovery on the ribbon. You can also right-click a VM and select Instant VM recovery. In this case, you will pass immediately to the Restore Point step of the wizard.
To quickly find a VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 2. Select VM**

At the **Virtual Machine** step of the wizard, select a VM that you want to restore.

1. In the **VM to recover** list, expand the necessary volume snapshot.
2. Select the VM.
To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 3. Select Restore Point**

At the **Restore Point** step of the wizard, select a restore point for the VM. Every storage snapshot acts as an independent restore point.
Step 4. Select Recovery Mode

At the **Recovery Mode** step of the wizard, specify the destination settings for recovered VMs.

1. Choose the restore mode:
   
   - Select **Restore to the original location** if you want to restore the VM with its initial settings to its original location. If you select this option, you will pass directly to the **Restore Reason** step of the wizard.
   
   - Select **Restore to a new location, or with different settings** if you want to restore the VM to a different location and/or with different settings. If you select this option, the **Instant Recovery** wizard will include additional steps for customizing VM settings.

2. Select the **Restore VM tags** check box if you want to restore tags that were assigned to the original VM, and assign them to the restored VM. Veeam Backup & Replication will restore the VM with original tags if the following conditions are met:
   
   - The VM is restored to its original location.
   
   - The original VM tag is still available on the source vCenter Server.

Step 5. Select Destination for Recovered VM

The **Destination** step of the wizard is available if you have chosen to change a location and settings of the recovered VM.

Select a destination for the recovered VM:

1. In the **Host** field, specify a host on which the VM must run. Veeam Backup & Replication will create a clone/virtual copy of the storage snapshot, mount it to the selected ESX(i) host and start the VM on this ESX(i) host.

2. In the **VM folder** field, select a folder to which you want to place the recovered VM.
3. In the **Restored VM name** field, enter a name under which the recovered VM must be registered. By default, Veeam Backup & Replication uses the original name of the VM. If you are restoring the VM to the same ESX(i) host or same datacenter where the original VM is registered, and the original VM still resides there, it is recommended that you change the VM name to avoid conflicts.

4. In the **Resource pool** list, select a resource pool to which you want to place the recovered VM.
Step 6. Specify Restore Reason

At the **Restore Reason** step of the wizard, enter a reason for performing Instant VM Recovery. The information you provide will be saved in the session history, and you will be able to view it later.

---

Step 7. Verify Instant VM Recovery Settings

At the **Ready to Apply** step of the wizard, specify additional settings for Instant VM Recovery:

1. If you are recovering a production VM that has failed and want to connect the recovered VM to a network upon restore, select the **Connect VM to network** check box. If you are recovering a VM for testing disaster recovery and the original VM is still running, leave this check box not selected. Before you power on the VM, you will have to manually change VM network configuration: disconnect it from the production network and connect it to an isolated non-production network to avoid conflicts.

2. To start the VM immediately after recovery, select the **Power on VM automatically** check box. If you are recovering the VM to the production network, make sure that the original VM is powered off to avoid conflicts.
3. Check Instant VM Recovery settings and click Next. Veeam Backup & Replication will restore the VM on the selected ESX(i) host.

---

**Step 8. Finalize Instant VM Recovery**

All currently running Instant VM Recovery sessions are displayed in the Home view, under the **Instant Recovery** node.

To check the progress of an Instant VM Recovery session and view session details:

1. Open the Home view.
2. In the inventory pane, click the Instant Recovery node.
3. In the working area, right-click the VM and select Properties.

Alternatively, you can open the History view, select the Instant Recovery node under Restore in the inventory pane and double-click the instant VM restore session.

After the VM has been successfully recovered, you can finalize Instant VM Recovery in one of two ways:

- Migrate the restored VM to the production environment
- Unpublish the recovered VM
Migrating Instantly Restored VMs

To migrate a recovered VM to the production environment:

1. Open the Home view.
2. In the inventory pane, select the Instant Recovery node.
3. In the working area, right-click the VM and select Migrate to production. Veeam Backup & Replication will launch the Quick Migration wizard.
   
   During migration, Veeam Backup & Replication will restore the VM from the backup file and additionally move all changes that were made while the VM was running from the backup in the Instant Recovery mode.

   **TIP:**

   When you pass though the Quick Migration wizard, enable the Delete source VM files upon successful migration option. Veeam Backup & Replication will restore the VM to production and automatically stop the Instant VM recovery session. If you do not enable this option, the Instant VM recovery session will still be running, and you will need to unpublish the recovered VM manually.

Unpublishing Instantly Restored VMs

If you have disabled the Delete source VM files upon successful migration option in the Quick Migration settings, you must unpublish the VM manually. After you unpublish the VM, the Instant Recovery session will end and the recovered VM will be unmounted from the vPower NFS server. The migrated VM will remain on the production environment.

To unpublish a recovered VM:

1. Open the Home view.
2. In the inventory pane, select the Instant Recovery node.
3. In the working area, right-click the VM and select Stop publishing.
TIP:

After the VM has been published from the backup, you can open the VM console directly from Veeam Backup & Replication. To do this, in the working area right-click the VM and select Open VM Console.
Restoring VM Guest OS Files (Microsoft Windows)

You can restore VM guest OS files from a storage snapshot. Veeam Backup & Replication supports file-level restore for the following Microsoft Windows file systems:

- FAT
- NTFS
- ReFS

When you perform guest OS file restore, you select an ESX(i) host in the virtual environment. Veeam Backup & Replication creates a clone of the storage snapshot on which the VM disks are hosted, and mounts the clone to the selected ESX(i) host as a new volume.

Veeam Backup & Replication accesses the configuration file of the VM (VMX) on the mounted clone and uses this configuration file to register a temporary VM on the ESX(i) host. Disks of the restored VM are mounted to this temporary VM. After disks are mounted, you can copy VM guest OS files and folders to their original location, local machine drive or save them in a network shared folder.

Before you start file-level restore, check prerequisites. Then use the File Level Restore wizard to restore VM guest OS files and folders.

1. Launch the File Level Restore wizard
2. Select a VM
3. Select a restore point
4. Select an ESX(i) host for snapshot mounting
5. Specify a restore reason
6. Save restored files

Before You Begin

Before you restore VM guest OS files from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- If you plan to restore VM guest OS files to their original location, you must make sure that VMware Tools are installed on the target VM.
- If you plan to restore guest OS files from a VM running Microsoft Windows ReFS, the Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later.
- If you plan to restore files from a VM running Microsoft Windows Server 2012 or later, and Data Deduplication is enabled for some VM volumes, the Veeam Backup & Replication console must be installed on a machine running Microsoft Windows Server 2012 or later. Data Deduplication must be enabled on this machine.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
• [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to the ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.

• [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch File Level Restore Wizard

To launch the **File Level Restore** wizard, do one of the following:

- On the **Home** tab, click **Restore** and select **VMware vSphere > Restore from backup > Guest files restore > Microsoft Windows**.

- Open the **Storage Infrastructure** view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM whose guest OS files you want to restore and click **Guest Files > Microsoft Windows** on the ribbon. You can also right-click a VM and select **Restore guest files > Microsoft Windows**. In this case, you will pass immediately to the **Location** step of the wizard.

- Open the **Home** view. In the inventory pane, select **Storage snapshots**. In the working area, expand the necessary volume, select a VM whose guest OS files you want to restore and click **Guest Files** > **Microsoft Windows** on the ribbon. You can also right-click a VM and select **Restore guest files** > **Microsoft Windows**. In this case, you will pass immediately to the **Restore Point** step of the wizard.

To quickly find the necessary VM, you can use the search field at the top of the window. Enter a VM name or a part of it and click the **Start search** button on the right or press [ENTER].

Step 2. Select VM

At the **Machine** step of the wizard, select a VM whose guest OS files you want to restore.

1. In the **VM to recover** list, expand the necessary volume snapshot.

2. Select the VM.
To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 3. Select Restore Point**

At the **Restore Point** step of the wizard, select a restore point for the VM. Every storage snapshot acts as an independent restore point.
Step 4. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup & Replication will create a temporary VM and mount disks of the restored VM to this temporary VM.

To specify destination for a snapshot clone/virtual copy and temporary VM:

1. At the **Location** step of the wizard, click **Customize**.
2. Next to the **Host** field, click **Choose** and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Next to the **Resource pool** field, click **Choose** and select a resource pool to which you want to place the temporary VM.
4. Next to the **VM folder** field, click **Choose** and select a folder to which you want to place the temporary VM.
5. Click **OK**.

Step 5. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for performing VM guest OS files restore. The information you provide will be saved in the session history, and you will be able to view it later.
**TIP:**

If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

---

**Step 6. Save Restored Files**

At the **Summary** step of the wizard, click **Finish** to start the restore process.

After the restore process is complete, Veeam Backup & Replication will open the Veeam Backup browser displaying the file system tree of the restored VM. Note that names of the restored VM hard disks may differ from the original ones.

You can perform the following operations with VM guest OS files in the Veeam Backup browser:

- Restore files and folders to the original location
- Save files and folders to a folder on the backup server or in network shared folder
- Launch Veeam Explorers for application item restore
- Open files in Microsoft Windows Explorer

After the restore process is complete, close the Veeam Backup browser.
Restoring Files to Original Location

To restore files or folders to their original location, in the Veeam Backup browser right-click a file or folder and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**.

Veeam Backup & Replication will add the "RESTORED" prefix to the original file name and store the restored file in the same folder where the original file resides.

If the file with the "RESTORED" prefix already exists in the original location, Veeam Backup & Replication will name the restored file in the following format: `RESTORED-<filename>__YYYYMMDD_HHMMSS`.

Saving Files to New Location

To save restored files or folders to a folder on the backup server or in a network shared folder, in the Veeam Backup browser right-click a file or folder and select **Copy To** and select a location to which the file or folder must be copied.

When restoring file objects, you can choose to preserve original NTFS permissions:

- Select the **Preserve permissions and ownership** check box to keep original ownership and security permissions for restored objects. Veeam Backup & Replication will copy files and folders with associated Access Control Lists and preserve granular access settings.
Leave the **Preserve permissions and ownership** check box not selected if you do not want to preserve original ownership and access settings for restored objects. Veeam Backup & Replication will change security settings: the user who launched the Veeam Backup & Replication console will be set as the owner of restored objects. Access permissions will be inherited from a folder to which restored objects are saved.

### Launching Veeam Explorers

If you are restoring VM guest OS files of the virtualized Microsoft Active Directory Server, Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft SQL Server, you can launch Veeam Explorer for the necessary application directly from the Veeam Backup browser.

- To start Veeam Explorer for Microsoft Active Directory, browse to the Microsoft Active Directory database file (DIT) in the Veeam Backup browser, select it and click Application Items > Active Directory Items on the Home tab or double-click the DIT file.

- To start Veeam Explorer for Microsoft Exchange, browse to the Microsoft Exchange database file (EDB) in the Veeam Backup browser, select it and click Application Items > Exchange Items on the Home tab or double-click the EDB file.

- To start Veeam Explorer for Microsoft SharePoint, browse to the Microsoft SharePoint content database (MDF) in the Veeam Backup browser, select it and click Application Items > SharePoint Items on the Home tab or double-click the MDF file.

- To start Veeam Explorer for Microsoft SQL Server, browse to the Microsoft SQL Server database file in the Veeam Backup browser, select it and click Application Items > SQL Server Databases on the Home tab or double-click the Microsoft SQL Server database file. For more information, see Microsoft Docs.
Working with Windows Explorer

You can use Microsoft Windows Explorer to work with restored files and folders.

To open Microsoft Windows Explorer:

1. In the Veeam Backup browser, click Explore on the ribbon or right-click the necessary folder and select Explore.

2. Veeam Backup & Replication will launch Microsoft Windows Explorer. Browse to the necessary VM guest OS files.

You can also start Microsoft Windows Explorer from the Start menu of Microsoft Windows and browse to the necessary VM guest OS files. VM disks are mounted under the C:\VeeamFLR\<vmname>\<volume n> folder on the backup server.

Closing Veeam Backup Browser

You can browse restored files and folders only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup & Replication unmounts VM disks from the temporary VM.

It is recommended that you close the Veeam Backup browser after you finish restoring files and folders.

Veeam Backup & Replication checks if there is any activity in the Veeam Backup browser every 5 minutes. If the user or Veeam Backup & Replication components and services do not perform any actions for 30 minutes, Veeam Backup & Replication displays a warning notifying that the Veeam Backup browser will be closed in 5 minutes.

After the warning is displayed, you can perform one of the following actions:

- You can close the Veeam Backup browser manually.
- You can click Cancel to postpone the close operation. The Veeam Backup browser will remain open for 5 minutes. After this period expires, Veeam Backup & Replication will display the warning again.
- You can perform no action. The Veeam Backup browser will be automatically closed in 5 minutes.
Restoring VM Guest OS Files (Linux, Unix and Other)

You can restore VM guest OS files from a storage snapshot. Veeam Backup & Replication supports file-level restore for the most commonly used file systems on Linux, Solaris, BSD, Unix and Micro Focus OES.

When you perform VM guest OS file restore, you select an ESX(i) host in your virtual environment. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot on which the VM disks are hosted, and mounts the clone/virtual copy to the selected ESX(i) host as a new volume.

Veeam Backup & Replication copies an ISO of the proxy appliance, a helper VM, to the mounted clone/virtual copy. The proxy appliance is rather small, around 50 MB. It requires 1024 MB RAM and takes 10-20 seconds to boot. Veeam Backup & Replication automatically starts the proxy appliance on the ESX(i) host and mounts disks of the restored VM to the proxy appliance as virtual hard drives. VMDK files are mounted directly from storage snapshots. After disks are mounted, you can copy necessary VM guest OS files and folders to their initial location, local machine drive or save them in a network shared folder.

Before you start file-level restore, check prerequisites. Then use the File Level Restore wizard to restore VM guest OS files and folders.

1. Launch the File Level Restore wizard
2. Select a VM
3. Select a restore point
4. Specify a restore reason
5. Select a location for the proxy appliance
6. Start the restore process
7. Save restored files

Before You Begin

Before you restore VM guest OS files from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- If you plan to restore VM guest OS files to their original location, make sure that VMware Tools must be installed on the target VM.
- Veeam Backup & Replication restores ACL for recovered VM guest OS files. To let Veeam Backup & Replication detect the target Linux system architecture and kernel version, make sure that the following utilities are installed on the VM guest OS: arch and uname.
- Veeam Backup & Replication must have access to the guest OS of the target VM to be able to deploy a coordination process. The coordination process performs a number of administrative actions on the target VM guest OS, for example, collects information about mount points.
For Linux target VM, mind the following:

- Veeam Backup & Replication uses the SSH protocol to communicate with the target Linux VM and requires the SCP utility on the target VM. Make sure that the SSH daemon is properly configured and SCP utility is available on the target VM.
- SELinux must be disabled on the target VM.
- A range of ports that are used for data transfer must be open on the target VM.
  
  [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.

- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system. For more information, see Required Licenses for NetApp.

Step 1. Launch File Level Restore Wizard

To launch the File Level Restore wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere > Restore from backup > Guest files restore > Linux and other.

- Open the Storage Infrastructure view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM whose guest OS files you want to restore and click Guest Files > Linux and other on the ribbon. You can also right-click a VM and select Restore guest files > Linux and other. In this case, you will pass immediately to the Restore Point step of the wizard.

- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM whose guest OS files you want to restore and click Guest Files > Linux and other on the ribbon. You can also right-click a VM and select Restore guest files > Linux and other. In this case, you will pass immediately to the Restore Point step of the wizard.

To quickly find a VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the Start search button on the right or press [ENTER].
Step 2. Select VM

At the Virtual Machine step of the wizard, select a VM whose guest OS files you want to restore.

1. In the Virtual machine list, expand the necessary volume snapshot.
2. Select the VM.

To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the Start search button on the right or press [ENTER].
Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point for the VM. Every storage snapshot acts as an independent restore point.
Step 4. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for performing VM guest OS files restore. The information you provide will be saved in the session history, and you will be able to view it later.

![Guest File Restore Wizard](image)

Step 5. Select Location for Proxy Appliance

At the **Ready** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup & Replication will also place a proxy appliance and mount disks of the restored VM to this proxy appliance.

To specify a destination for the snapshot clone/virtual copy and proxy appliance:

1. Click the **Customize** link at the bottom of the window.
2. In the **FLR Appliance Configuration** window, select an ESX(i) host to which the snapshot clone must be mounted and on which the proxy appliance must be registered.
3. In the **Resource pool** field, specify a resource pool to which you want to place the proxy appliance.
4. In the **Network** section, specify an IP address and other network settings for the proxy appliance. The proxy appliance must be placed in the same network where the backup server resides.
5. To enable FTP access to the restored file system, select the **Enable FTP server on appliance** check box. As a result, your users will be able to access the proxy appliance via FTP, browse the file system of the restored VM and download files on their own.
6. If you are restoring a VM with the Novell Storage Services file system, select the **Restore from Novell Storage Services (NSS) file system** check box. Veeam Backup & Replication will deploy a specific proxy appliance that supports the Novell Storage Services file system.
7. Click **OK**.
IMPORTANT!

When choosing an ESX(i) host for the proxy appliance used for file-level restore from the Novell Storage Services file system, make sure that it allows running VMs with 64-bit guest OSes.
Step 6. Start Restore Process

At the **Restore** step of the wizard, check the progress of the restore process. The file-level restore appliance may take about 10-20 seconds to boot.

![Guest File Restore Wizard](image)

Step 7. Save Restored Files

When the restore process is complete, Veeam Backup & Replication opens the Veeam Backup browser displaying the file system tree of the restored VM.

You can restore files and folders to their original location, new location or access files on FTP.

**NOTE:**

You can browse to the VM guest OS files and access restored files on the FTP only while the Veeam Backup browser is open. After the Veeam Backup browser is closed, Veeam Backup & Replication will unmount VM disks from the proxy appliance, remove the proxy appliance and unmount the storage snapshot from the ESX(i) host (unless this storage snapshot is used by other restore operations).

**Restoring Files to Original Location**

To restore files and folders to the original location, in the Veeam Backup browser right-click a file or folder and select one of the following commands:

- To overwrite the original file on the VM guest OS with the file restored from the backup, select **Restore > Overwrite**.
- To save the file restored from the backup next to the original file, select **Restore > Keep**.

Veeam Backup & Replication will add the `.RESTORED-YYYYMMDDHHMMSS` suffix to the original file name and store the restored file in the same folder where the original file resides.
To access the target VM guest OS and restore files to the original location, Veeam Backup & Replication uses an account specified in the backup job settings. If this account does not have sufficient rights to access the target VM guest OS, you will be prompted to enter credentials. In the **Credentials window**, specify a user account to access the destination location (server or shared folder). You can use the account under which you are currently logged on or a different account.

In some cases, you may remove the original VM and restore it from the backup by the time of file-level restore. If you then attempt to restore VM guest OS files to the original location, Veeam Backup & Replication will not be able to find the original VM by its reference ID, and display a warning. Click **OK** and browse to the target VM in the virtual infrastructure to which you want to restore VM guest OS files.

**Saving Files to New Location**

To save files and folders to a new location:

1. In the Veeam Backup browser, right-click the necessary file or folder and select **Copy to**.
2. In the **Select Destination** window, select a destination server (local or remote) from the list or provide a path to a shared folder.
   - If you are recovering files to a Linux server, you can select the destination server from the list or add the destination server ad-hoc. To add a destination server ad-hoc, scroll down the list of servers and choose **Specify a different host** at the end of the list. Follow the steps of the wizard to add a Linux server that will be used as the destination server.

   The server you add ad-hoc will not appear in the list of managed hosts in Veeam Backup & Replication: its purpose is to host files that you recover. The added server will only remain visible in the Veeam Backup browser until all currently active file-level restore sessions are completed.

   - If you are recovering files to a shared folder, specify a path to the destination folder.
3. If you want to preserve original permissions and ownership for recovered files, select the **Preserve permissions and ownership** check box.

4. After you click **Restore**, you may need to specify credentials to access the destination location. If prompted, in the **Credentials** window specify the user account to access the target server or shared folder. You can use the account under which you are currently logged on or a different account.

**IMPORTANT!**

If you plan to keep original permissions and ownership settings of restored files and folders, the account you specify must have privileges to change the owner on the target server or in the shared folder.

---

**Accessing Files over FTP**

If you have chosen to enable an FTP server on the FLR appliance, the restored file system will also be available over FTP at `ftp://<FLR_appliance_IP_address>`. Users in the same network can access the FLR appliance and restore files they need on their own.
Restoring Application Items from Microsoft Active Directory

Veeam Backup & Replication integrates with Veeam Explorer for Microsoft Active Directory. Veeam Explorer for Microsoft Active Directory lets you browse Microsoft Active Directory databases in VMs located on storage snapshots and restore Microsoft Active Directory items (objects and containers) and their attributes back to the production Microsoft Active Directory database.

Before you start working with Veeam Explorer for Microsoft Active Directory, you need to extract a Microsoft Active Directory database from the storage snapshot. You can do it in two ways:

- You can use the **Microsoft Active Directory Object Restore** wizard. In this case, Veeam Backup & Replication will automatically extract a Microsoft Active Directory database from the storage snapshot and open it in Veeam Explorer for Microsoft Active Directory. For more information, see [Using Microsoft Active Directory Object Restore Wizard](#).

- You can restore VM guest OS files from a backup of a virtualized Microsoft Active Directory server, manually locate a Microsoft Active Directory database and open it in Veeam Explorer for Microsoft Active Directory. For more information, see [Opening Microsoft Active Directory Database Manually](#).

**Using Microsoft Active Directory Object Restore Wizard**

When you run the **Microsoft Active Directory Object Restore** wizard, Veeam Backup & Replication automatically extracts the Microsoft Active Directory database from the storage snapshot and opens it in Veeam Explorer for Microsoft Active Directory.

As part of this procedure, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to an ESX(i) host.
2. Veeam Backup & Replication accesses the configuration file of the virtualized Microsoft Active Directory server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup & Replication mounts disks of the Microsoft Active Directory server to the temporary VM.

Before you restore the Microsoft Active Directory database from a storage snapshot, check prerequisites. Then use the **Microsoft Active Directory Object Restore** wizard to restore the Microsoft Active Directory database.

1. Launch the Microsoft Active Directory Object Restore wizard
2. Select a VM
3. Select a restore point
4. Select an ESX(i) host for snapshot mounting
5. Specify a restore reason
6. Open the database in Veeam Explorer for Microsoft Active Directory
Before You Begin

Before you restore application items from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch Microsoft Active Directory Object Restore Wizard

To launch the Microsoft Active Directory Restore wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere > Restore from backup or Restore from replica > Application items restore > Microsoft Active Directory.

- Open the Storage Infrastructure view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM running Microsoft Active Directory and click Application Items > Microsoft Active Directory on the ribbon. You can also right-click the VM and select Restore application items > Microsoft Active Directory objects. In this case, you will pass immediately to the Location step of the wizard.

- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM running Microsoft Active Directory and click Application Items > Microsoft Active Directory on the ribbon. You can also right-click the VM and select Restore application items > Microsoft Active Directory objects. In this case, you will pass immediately to the Restore Point step of the wizard.
To quickly find a VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

Step 2. Select VM

At the **Machines** step of the wizard, Veeam Backup & Replication displays all Microsoft Active Directory VMs whose disks are located on the storage system. Select the necessary VM from the list. If the necessary VM is not displayed in the list, select the **Show all VMs** check box. Veeam Backup & Replication will display all VMs whose disks are located on the storage system.
To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 3. Select Restore Point**

At the **Restore Point** step of the wizard, select a restore point from which you want to restore a Microsoft Active Directory database. Every storage snapshot acts as an independent restore point.
Step 4. Select ESX(i) Host for Snapshot Mounting

At the Location step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup & Replication will create a temporary VM and mount disks of the virtualized Microsoft Active Directory to this temporary VM.

To specify a destination for the snapshot clone/virtual copy and temporary VM:

1. At the Location step of the wizard, click Customize.
2. Next to the Host field, click Choose and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Next to the Resource pool field, click Choose and select a resource pool to which you want to place the temporary VM.
4. Next to the Folder field, click Choose and select a folder to which you want to place the temporary VM.
5. Click OK.

Step 5. Specify Restore Reason

At the Reason step of the wizard, enter a reason for restoring a Microsoft Active Directory database. The information you provide will be saved in the session history, and you will be able to view it later.
**TIP:**

If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

---

**Step 6. Open Database in Veeam Explorer for Microsoft Active Directory**

At the **Summary** step of the wizard, click **Finish** to start the restore process.

Veeam Backup & Replication will automatically locate a Microsoft Active Directory database and open it in Veeam Explorer for Microsoft Active Directory. You can browse the database and restore items that you need.
Detailed information about Veeam Explorer for Microsoft Active Directory is provided in documentation for Veeam Explorer for Microsoft Active Directory. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft Active Directory and press [F1].
- From the main menu of Veeam Explorer for Microsoft Active Directory, select Help > Online Help.

Opening Microsoft Active Directory Database Manually

If Veeam Backup & Replication fails to locate a Microsoft Active Directory database automatically for some reason, you can use the file-level restore functionality to restore a Microsoft Active Directory database from the storage snapshot. You can then open the database in Veeam Explorer for Microsoft Active Directory.

To restore application items from Microsoft Active Directory:

1. Restore VM guest OS files from a backup of a virtualized Microsoft Active Directory server. For more information, see Restoring VM Guest OS Files (Microsoft Windows).

2. In the Veeam Backup browser, locate a Microsoft Active Directory database file (NTDS.dit) and double-click it or select the NTDS.dit file and click Application Items > Microsoft Active Directory on the ribbon.

Veeam Backup & Replication will open the database in Veeam Explorer for Microsoft Active Directory. After that, you can browse the database and restore Microsoft Active Directory objects.
Detailed information about Veeam Explorer for Microsoft Active Directory is provided in documentation for Veeam Explorer for Microsoft Active Directory. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft Active Directory and press [F1].
- Open Veeam Explorer for Microsoft Active Directory. From the main menu of Veeam Explorer for Microsoft Active Directory, select Help > Online Help.
Restoring Application Items from Microsoft Exchange

Veeam Backup & Replication integrates with Veeam Explorer for Microsoft Exchange. Veeam Explorer for Microsoft Exchange lets you browse Microsoft Exchange mailbox stores in VMs located on storage snapshots and restore Microsoft Exchange items that you need.

Before you start working with Veeam Explorer for Microsoft Exchange, you need to extract a Microsoft Exchange database (an EDB file) from the storage snapshot. You can do it in two ways:

- You can use the **Microsoft Exchange Item Level Restore** wizard. In this case, Veeam Backup & Replication will automatically extract a Microsoft Exchange database from the storage snapshot and open it in Veeam Explorer for Microsoft Exchange. For more information, see Using the Microsoft Exchange Item Level Restore Wizard.

- You can restore VM guest OS files from a backup of a virtualized Microsoft Exchange server, manually locate a Microsoft Exchange database and open it in Veeam Explorer for Microsoft Exchange. For more information, see Opening Microsoft Exchange Database Manually.

Using the Microsoft Exchange Item Level Restore Wizard

When you run the **Microsoft Exchange Item Level Restore** wizard, Veeam Backup & Replication automatically extracts a Microsoft Exchange database (an EDB file) from the storage snapshot and opens it in Veeam Explorer for Microsoft Exchange.

As part of this procedure, Veeam Backup & Replication performs the following steps:

1. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to an ESX(i) host.
2. Veeam Backup & Replication accesses the configuration file of the virtualized Microsoft Exchange server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup & Replication mounts disks of the Microsoft Exchange server to the temporary VM.
5. Veeam Backup & Replication opens the EDB file in Veeam Explorer for Exchange, and you can browse it to find necessary items.

Before you restore Microsoft Exchange objects from a storage snapshot, check prerequisites. Then use the **Microsoft Exchange Item Level Restore** wizard to restore the Microsoft Exchange database.

1. Launch the Microsoft Exchange Item Level Restore wizard
2. Select a VM
3. Select a restore point
4. Select an ESX(i) host for snapshot mounting
5. Specify a restore reason
6. Open the EDB file in Veeam Explorer for Exchange
Before You Begin

Before you restore application items from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch Microsoft Exchange Item Level Restore Wizard

To launch the Microsoft Exchange Item Level Restore wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere > Restore from backup or Restore from replica > Application items restore > Microsoft Exchange.

- Open the Storage Infrastructure view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM running Microsoft Exchange and click Application Items > Microsoft Exchange on the ribbon. You can also right-click the VM and select Restore application items > Microsoft Exchange mailbox items. In this case, you will pass immediately to the Location step of the wizard.

- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM running Microsoft Exchange and click Application Items > Microsoft Exchange on the ribbon. You can also right-click the VM and select Restore application items > Microsoft Exchange mailbox items. In this case, you will pass immediately to the Restore Point step of the wizard.
To quickly find the necessary VM, you can use the search field at the top of the window. Enter a VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 2. Select VM**

At the **Machines** step of the wizard, Veeam Backup & Replication displays all Microsoft Exchange VMs with disks whose disks are located on the storage system. Select the necessary VM in the list. If the necessary VM is not displayed in the list, select the **Show all VMs** check box. Veeam Backup & Replication will display all VMs whose disks are located on the storage system.
To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press **[ENTER]**.

**Step 3. Select Restore Point**

At the **Restore Point** step of the wizard, select a restore point from which you want to recover a Microsoft Exchange database. Every storage snapshot acts as an independent restore point.
Step 4. Select ESX(i) Host for Snapshot Mounting

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot will be mounted. On the selected ESX(i) host, Veeam Backup & Replication will create a temporary VM and mount disks of the virtualized Microsoft Exchange server to this temporary VM.

To specify a destination for the snapshot clone/virtual copy and temporary VM:

1. At the **Location** step of the wizard, click **Customize**.
2. Next to the **Host** field, click **Choose** and select an ESX(i) host to which the snapshot clone must be mounted and on which the temporary VM must be created.
3. Next to the **Resource pool** field, click **Choose** and select a resource pool to which you want to place the temporary VM.
4. Next to the **Folder** field, click **Choose** and select a folder to which you want to place the temporary VM.
5. Click **OK**.

Step 5. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring data from Microsoft Exchange. The information you provide will be saved in the session history, and you will be able to view it later.
TIP:
If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

**Step 6. Open EDB File in Veeam Explorer for Exchange**

At the **Summary** step of the wizard, click **Finish** to start the restore process.

Veeam Backup & Replication will automatically locate a Microsoft Exchange database and open it in Veeam Explorer for Microsoft Exchange. You can browse the database and restore items that you need.
Detailed information about Veeam Explorer for Microsoft Exchange is provided in documentation for Veeam Explorer for Microsoft Exchange. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft Exchange and press [F1].
- From the main menu of Veeam Explorer for Microsoft Exchange, select Help > Online Help.

Opening Microsoft Exchange Database Manually

If Veeam Backup & Replication fails to locate a Microsoft Exchange database automatically for some reason, you can use the file-level restore functionality to restore a Microsoft Exchange database from the storage snapshot. You can then open the database in Veeam Explorer for Microsoft Exchange.

To restore application items from Microsoft Exchange:

1. Restore VM guest OS files from a backup of a virtualized Microsoft Exchange server. For more information, see Restoring VM Guest OS Files (Microsoft Windows).
2. In the Veeam Backup browser, locate an EDB file and double-click it or select the EDB file and click Application Items > Microsoft Exchange on the ribbon.

Veeam Backup & Replication will open the selected database in Veeam Explorer for Microsoft Exchange. After that, you can browse the database and restore items that you need.
Detailed information about Veeam Explorer for Microsoft Exchange is provided in documentation for Veeam Explorer for Microsoft Exchange. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft Exchange and press [F1].
- Open Veeam Explorer for Microsoft Exchange. From the main menu of Veeam Explorer for Microsoft Exchange, select Help > Online Help.
Restoring Application Items from Microsoft SharePoint

Veeam Backup & Replication integrates with Veeam Explorer for Microsoft SharePoint. Veeam Explorer for Microsoft SharePoint lets you browse Microsoft SharePoint content databases in VMs located on storage snapshots and restore documents, items and document libraries that you need.

Before you start working with Veeam Explorer for Microsoft SharePoint, you need to extract a Microsoft SharePoint content database (an MDF file) from the storage snapshot. To do this, you need to restore VM guest OS files from a backup of the virtualized Microsoft SharePoint server, manually locate the content database and open it in Veeam Explorer for Microsoft SharePoint.

To restore application items from Microsoft SharePoint:

1. Restore VM guest OS files from a backup of a virtualized Microsoft SharePoint server. For more information, see Restoring VM Guest OS Files (Microsoft Windows).

2. In the Veeam Backup browser, locate the MDF file and double-click it or select the file and click Application Items > Microsoft SharePoint on the ribbon.

Veeam Backup & Replication will attach the content database to the Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed and open the database in Veeam Explorer for Microsoft SharePoint. After that, you can browse the database and restore items that you need.
Detailed information about Veeam Explorer for Microsoft SharePoint is provided in documentation for Veeam Explorer for Microsoft SharePoint. To open access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft SharePoint and press [F1].
- From the main menu of Veeam Explorer for Microsoft SharePoint, select Help > Online Help.
Restoring Databases from Microsoft SQL Server

Veeam Backup & Replication integrates with Veeam Explorer for Microsoft SQL Server. Veeam Explorer for Microsoft SQL Server lets you browse Microsoft SQL Server databases in VMs located on storage snapshots and restore Microsoft SQL Server databases.

Before you start working with Veeam Explorer for Microsoft SQL Server, you need to extract the Microsoft SQL Server database from the storage snapshot. You can do it in two ways:

- You can use the Microsoft SQL Server Database Restore wizard. In this case, Veeam Backup & Replication will automatically extract a Microsoft SQL Server database from the storage snapshot and open it in Veeam Explorer for Microsoft SQL. For more information, see Using the Microsoft SQL Server Database Restore Wizard.

- You can restore VM guest OS files from a backup of a virtualized Microsoft SQL Server, manually locate a Microsoft SQL Server database and open it in Veeam Explorer for Microsoft SQL Server. For more information, see Opening Microsoft SQL Server Database Manually.

Using the Microsoft SQL Server Database Restore Wizard

When you run the Microsoft SQL Server Database Restore wizard, Veeam Backup & Replication automatically extracts a Microsoft SQL Server database from the storage snapshot and opens it in Veeam Explorer for Microsoft SQL Server.

As part of this procedure, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to an ESX(i) host.
2. Veeam Backup & Replication accesses the configuration file of the virtualized Microsoft SQL Server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.
3. Veeam Backup & Replication mounts disks of the Microsoft SQL Server to the temporary VM.
4. Veeam Backup & Replication locates a Microsoft SQL Server database and attaches the content database to a staging Microsoft SQL Server. As a staging server, Veeam Backup & Replication uses the Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed.
5. Veeam Backup & Replication opens the database in Veeam Explorer for Microsoft SQL Server.

Before you restore Microsoft SQL Server databases from the storage snapshot, check prerequisites. Then use the Microsoft SQL Server Database Restore wizard to restore Microsoft SQL Server databases.

1. Launch the Microsoft SQL Server Database Restore wizard
2. Select a VM
3. Select a restore point
4. Select an ESX(i) host for snapshot mounting
5. Specify a restore reason
6. Open the database in Veeam Explorer for Microsoft SQL
Before You Begin

Before you restore application items from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch Microsoft SQL Server Database Restore Wizard

To launch the Microsoft SQL Server Database Restore wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere > Restore from backup or Restore from replica > Application items restore > Microsoft SQL Server.

- Open the Storage Infrastructure view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM running Microsoft SQL Server and click Application Items > Microsoft SQL Server on the ribbon. You can also right-click the VM and select Restore application items > Microsoft SQL Server databases. In this case, you will pass immediately to the Location step of the wizard.

- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM running Microsoft SQL Server and click Application Items > Microsoft SQL Server on the ribbon. You can also right-click the VM and select Restore application items > Microsoft SQL Server databases. In this case, you will pass immediately to the Restore Point step of the wizard.

To quickly find the necessary VM, you can use the search field at the top of the window. Enter a VM name or a part of it and click the Start search button on the right or press [ENTER].
Step 2. Select VM

At the **Machines** step of the wizard, Veeam Backup & Replication displays all Microsoft SQL Server VMs whose disks are located on the storage system. Select the necessary VM in the list. If the necessary VM is not displayed in the list, select the **Show all VMs** check box. Veeam Backup & Replication will display all VMs whose disks are located on the storage system.

To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press `[ENTER]`.

---

**Microsoft SQL Server Database Restore**

**Machines**
Select a SQL server machine to restore from.

**SQL server: hpvsad1**

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Job name</th>
<th>Latest restore point</th>
<th>Restore points count</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpvsad1</td>
<td>exSQL-dhlhpvsad (ex...</td>
<td>2/2/2019 10:01:25 AM</td>
<td>4</td>
</tr>
</tbody>
</table>

---

Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to restore a Microsoft SQL Server database. Every storage snapshot acts as an independent restore point.

- Select **Restore from the latest available backup** if you want to restore a database from the latest restore point in the backup chain.
• Select **Restore from this restore point** if you want to restore a database from a specific restore point.

![Microsoft SQL Server Database Restore](image)

**Step 4. Select ESX(i) Host for Snapshot Mounting**

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup & Replication will create a temporary VM and mount disks of the virtualized Microsoft SQL Server to this temporary VM.

To specify a destination for the snapshot clone/virtual copy and temporary VM:

1. At the **Location** step of the wizard, click **Customize**.
2. Next to the **Host** field, click **Choose** and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Next to the **Resource pool** field, click **Choose** and select a resource pool to which you want to place the temporary VM.
4. Next to the **Folder** field, click **Choose** and select a folder to which you want to place the temporary VM.
5. Click OK.

Microsoft SQL Server Database Restore

Location
Specify where the location where a temporary VM should be registered. This VM will remain powered off and will be automatically removed once the restore process completes.

Machines
Review the restore settings:

Restore Point

Location
Reason
Summary

Restore Configuration

Specify a host to mount storage snapshot to, as well as resource pool and VM folder for temporary VM. Once you finish restoring, the wizard will perform clean up automatically.

Host:
exe11tech.local

Resource pool:

VM folder:

After you click Next, the wizard will mount a clone of the selected snapshot to the specified host as a new datastore, and register the VM with virtual infrastructure.

Customize

< Previous  Next >  Finish  Cancel
Step 5. Specify Restore Reason

At the Reason step of the wizard, enter a reason for restoring a database from the Microsoft SQL Server VM. The information you provide will be saved in the session history, and you will be able to view it later.

**TIP:**

If you do not want to display the Reason step of the wizard in future, select the Do not show me this page again check box.

Step 6. Open Database in Veeam Explorer for Microsoft SQL Server

At the Summary step of the wizard, click Finish to start the restore process.

Veeam Backup & Replication will automatically locate a Microsoft SQL Server database and attach the content database to a staging Microsoft SQL Server. After that, Veeam Backup & Replication will open the Veeam Explorer for Microsoft SQL Server and add the restored database to it.
Detailed information about Veeam Explorer for Microsoft SQL is provided in documentation for Veeam Explorer for Microsoft SQL. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft SQL Server and press [F1].
- Open Veeam Explorer for Microsoft SQL Server. From the main menu of Veeam Explorer for Microsoft SQL Server, select Help > Online Help.

Opening Microsoft SQL Server Database Manually

If Veeam Backup & Replication fails to locate a Microsoft SQL Server database automatically for some reason, you can use the file-level restore functionality to restore a Microsoft SQL Server database from the storage snapshot. You can then open the database in Veeam Explorer for Microsoft SQL Server.

To restore a Microsoft SQL Server database:

1. Restore VM guest OS files from a backup of a virtualized Microsoft SQL Server. For more information, see Restoring VM Guest OS Files (Microsoft Windows).

2. In the Veeam Backup browser, locate the MDF file and double-click it or select the file and click Application Items > Microsoft SQL Server on the ribbon.

Veeam Backup & Replication will attach the restored database to the Microsoft SQL Server on which the Veeam Backup & Replication configuration database is deployed and open the database in Veeam Explorer for Microsoft SQL Server. After that, you can restore the database to the necessary Microsoft SQL Server.
Detailed information about Veeam Explorer for Microsoft SQL is provided in documentation for Veeam Explorer for Microsoft SQL. To access the documentation, do one of the following:

- Open Veeam Explorer for Microsoft SQL Server and press [F1].
- Open Veeam Explorer for Microsoft SQL Server. From the main menu of Veeam Explorer for Microsoft SQL Server, select Help > Online Help.
Restoring Databases from Oracle

Veeam Backup & Replication integrates with Veeam Explorer for Oracle — a tool that lets you browse Oracle databases in VMs located on storage snapshots and restore Oracle databases.

Before you start working with Veeam Explorer for Oracle, you need to extract an Oracle database from the storage snapshot. You can do it in two ways:

- You can use the Oracle Database Restore wizard. In this case, Veeam Backup & Replication will automatically extract an Oracle database from the storage snapshot and open it in Veeam Explorer for Oracle. For more information, see Using the Oracle Database Restore Wizard.

- You can restore VM guest OS files from a backup of a virtualized Oracle server, manually locate an Oracle database and open it in Veeam Explorer for Oracle. For more information, see Opening Oracle Database Manually.

Using the Oracle Restore Wizard

When you run the Oracle Database Restore wizard, Veeam Backup & Replication automatically extracts an Oracle database from the storage snapshot and opens it in Veeam Explorer for Oracle.

As part of this procedure, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication creates a clone/virtual copy of the storage snapshot and mounts the clone/virtual copy to an ESX(i) host.

2. Veeam Backup & Replication accesses the configuration file of the virtualized Oracle server (VMX) on the snapshot clone/virtual copy and uses this configuration file to register a temporary VM on the ESX(i) host.

3. Veeam Backup & Replication mounts disks of the Oracle server to the temporary VM.

4. Veeam Backup & Replication locates the Oracle database and attaches the database to a staging Oracle server.

5. Veeam Backup & Replication opens the database in Veeam Explorer for Oracle.

Before you restore an Oracle database from the storage snapshot, check prerequisites. Then use the Oracle Database Restore wizard to restore the Oracle database.

1. Launch the Oracle Database Restore wizard

2. Select a VM

3. Select a restore point

4. Select an ESX(i) host for snapshot mounting

5. Specify a restore reason

6. Open the database in Veeam Explorer for Oracle
Before You Begin

Before you restore application items from storage snapshots, check the following prerequisites:

- You must add the storage system to the backup infrastructure.
- You must check limitations for Veeam Explorer for Storage Snapshots. For more information, see Veeam Explorer for Storage Snapshots.
- [For storage systems working over Fibre Channel] To let Veeam Backup & Replication present snapshots of LUNs to an ESX(i) host, you must register the ESX(i) host with a WWN ID on the storage system.
- [For NetApp storage systems] Depending on the storage type, you may need to install additional licenses on the storage system.

Step 1. Launch Oracle Database Restore Wizard

To launch the Oracle Database Restore wizard, do one of the following:

- On the Home tab, click Restore and select VMware vSphere > Restore from backup or Restore from replica > Application items restore > Oracle Database.
- Open the Storage Infrastructure view. In the inventory pane, select the necessary volume snapshot. In the working area, select a VM running Oracle and click Application Items > Oracle on the ribbon. You can also right-click the VM and select Restore application items > Oracle databases. In this case, you will pass immediately to the Location step of the wizard.
- Open the Home view. In the inventory pane, select Storage snapshots. In the working area, expand the necessary volume, select a VM running Oracle and click Application Items > Oracle on the ribbon. You can also right-click the VM and select Restore application items > Oracle databases. In this case, you will pass immediately to the Restore Point step of the wizard.

To quickly find a VM, you can use the search field at the top of the window. Enter the VM name or a part of it and click the Start search button on the right or press [ENTER].
Step 2. Select VM

At the **Virtual Machine** step of the wizard, Veeam Backup & Replication displays all Oracle VMs whose disks are located on the storage system. Select the necessary VM in the list. If the necessary VM is not displayed in the list, select the **Show all VMs** check box. Veeam Backup & Replication will display all VMs whose disks are located on the storage system.

To quickly find a VM, you can use the search field at the bottom of the window. Enter the VM name or a part of it and click the **Start search** button on the right or press [ENTER].

---

Step 3. Select Restore Point

At the **Restore Point** step of the wizard, select a restore point from which you want to restore an Oracle database. Every storage snapshot acts as an independent restore point.

- Select **Restore from the latest available backup** if you want to restore a database from the latest restore point in the backup chain.
• Select **Restore from this restore point** if you want to restore a database from a specific restore point.

![Oracle Database Restore](image)

**Step 4. Select ESX(i) Host for Snapshot Mounting**

At the **Location** step of the wizard, select an ESX(i) host to which the clone/virtual copy of the storage snapshot must be mounted. On the selected ESX(i) host, Veeam Backup & Replication will create a temporary VM and mount the disks of the virtualized Oracle server to this temporary VM.

To specify a destination for the snapshot clone/virtual copy and temporary VM:

1. At the **Location** step of the wizard, click **Customize**.
2. Next to the **Host** field, click **Choose** and select an ESX(i) host to which the snapshot clone/virtual copy must be mounted and on which the temporary VM must be created.
3. Next to the **Resource pool** field, click **Choose** and select a resource pool to which you want to place the temporary VM.
4. Next to the **Folder** field, click **Choose** and select a folder to which you want to place the temporary VM.
5. Click OK.
Step 5. Specify Restore Reason

At the **Reason** step of the wizard, enter a reason for restoring a database from the Oracle VM if necessary. The information you provide will be saved in the session history, and you will be able to view it later.

**TIP:**

If you do not want to display the **Reason** step of the wizard in future, select the **Do not show me this page again** check box.

Step 6. Open Database in Veeam Explorer for Oracle

At the **Summary** step of the wizard, click **Finish** to start the restore process.

Veeam Backup & Replication will automatically locate an Oracle database and attach the content database to the staging server. After that, Veeam Backup & Replication will open the Veeam Explorer for Oracle and add the database to it.
Detailed information about Veeam Explorer for Oracle is provided in documentation for Veeam Explorer for Oracle. To access the documentation, do one of the following:

- Open Veeam Explorer for Oracle and press [F1].
- Open Veeam Explorer for Oracle. From the main menu of Veeam Explorer for Oracle, select Help > Online Help.

Opening Oracle Database Manually

If Veeam Backup & Replication fails to locate an Oracle database automatically for some reason, you can use the file-level restore functionality to restore an Oracle database from the storage snapshot. You can then open the database in Veeam Explorer for Oracle.

To restore an Oracle database:

1. Restore VM guest OS files from a backup of a virtualized Oracle server. For more information, see Restoring VM Guest OS Files (Microsoft Windows).

2. In the Veeam Backup browser, locate the database file and double-click it or select the file and click Application Items > Oracle on the ribbon.

Veeam Backup & Replication will attach the restored database to a staging server and open the database in Veeam Explorer for Oracle. After that, you can restore the database to the necessary Oracle server.
Detailed information about Veeam Explorer for Oracle is provided in documentation for Veeam Explorer for Oracle. To access the documentation, do one of the following:

- Open Veeam Explorer for Oracle and press [F1].
- Open Veeam Explorer for Oracle. From the main menu of Veeam Explorer for Oracle, select **Help > Online Help.**
On-Demand Sandbox for Storage Snapshots

In the On-Demand Sandbox, you can start VMs from snapshots existing on the production storage array. You can use the On-Demand Sandbox to test VMs, troubleshoot issues, perform training and so on.

Veeam Backup & Replication offers the On-Demand Sandbox functionality for the following storage systems:

- Dell EMC VNX(e)\Unity
- HPE 3PAR StoreServ, including secondary volumes — HPE 3PAR Peer Persistence
- HPE StoreVirtual P4000 series and HPE StoreVirtual VSA (Virtual Storage Appliance)
- IBM Spectrum Virtualize, including secondary IBM volumes — IBM Spectrum Virtualize HyperSwap
- NetApp, including secondary arrays — NetApp SnapMirror and NetApp SnapVault
- HPE Nimble storage, including secondary arrays — Nimble Snapshot Replicated Copy
- Universal Storage API Integrated Systems

Configuration of the On-Demand Sandbox in which VMs from storage snapshots are started is similar to configuration of the regular On-Demand Sandbox. To start a VM from the storage snapshot in the isolated environment, you must configure the following objects:

- **Virtual lab.** The virtual lab must mirror the networking scheme of the production environment. You can configure a new virtual lab or use an existing virtual lab. Any type of the virtual lab configuration is supported: basic single-host, advanced single-host or advanced multi-host. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.

- **Application group.** The application group must contain one or several VMs that you want to start in the On-Demand Sandbox. You can select VMs from volumes or LUNs on the storage system. During the SureBackup job, Veeam Backup & Replication will detect the latest snapshot for this volume or LUN and start the VM from this snapshot. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.

- **SureBackup job.** You must link the application group with VMs and virtual lab to the SureBackup job. For more information, see Veeam Backup & Replication User Guide for VMware vSphere.

How On-Demand Sandbox for Storage Snapshots Works

To start a VM from the storage snapshot in the On-Demand Sandbox, Veeam Backup & Replication needs to present this storage snapshot to an ESX(i) host as a datastore. To do this, Veeam Backup & Replication performs the following actions:

1. Veeam Backup & Replication detects the latest storage snapshot for the VM whose disks are located on the storage system.
2. Veeam Backup & Replication triggers the storage system to create a copy of the storage snapshot. The snapshot copy helps protect the storage snapshot from changes.

To create a snapshot copy, Veeam Backup & Replication uses the same technology as for Veeam Explorer from Storage Snapshots. The technology choice depends on licenses installed on the storage system. For more information, see Veeam Explorer for Storage Snapshots.
3. The snapshot copy is presented as a new datastore to the ESX(i) host on which the virtual lab is registered.

4. Veeam Backup & Replication performs regular operations required for On-Demand Sandbox: reconfigures the VMX file, starts the VM, performs necessary tests for it and so on.

5. After you finish working with VMs and power off the On-Demand Sandbox, Veeam Backup & Replication performs cleanup operations: powers off the VM and the proxy appliance in the virtual lab, unmounts the datastore from the ESX(i) host and triggers the storage system to remove the snapshot copy.

Number of Mounted NFS Datastores

You can add to the application group several VMs that reside on different storage snapshots. In this case, Veeam Backup & Replication will trigger several snapshot copies (one per each storage snapshot) and present the equal number of datastores to the ESX(i) host.

The number of NFS datastores that can be mounted to the ESX(i) host is limited by VMware vSphere. If number of snapshot copies is great, Veeam Backup & Replication may fail to present all of them as datastores to the ESX(i) host. In this case, VMs in the application group will not be started and the SureBackup job will fail. For more information about limitations, see this VMware KB article.

To overcome this situation, Veeam Backup & Replication offers the mechanism of the snapshot copy re-mounting:

1. If Veeam Backup & Replication detects that there are not enough resources to mount a datastore, it displays a warning and offers you to free up resources on the ESX(i) host.

2. During the next 20 minutes, Veeam Backup & Replication attempts to mount the datastore with the time interval of 2 minutes.

3. If resources are freed and Veeam Backup & Replication manages to mount the datastore, VMs in the application group are started and the SureBackup job continues to run. If resources on the ESX(i) hosts are not freed within 20 minutes, the SureBackup job fails.

Limitations for On-Demand Sandbox for Storage Snapshots

Before you start using On-Demand Sandbox for storage snapshots, check limitations for Veeam Explorer for Storage Snapshots. For more information, see General Limitations.
Requirements and Limitations

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots have a set of limitations and requirements to storage systems.

- System Requirements
- General Limitations
- Limitations for Cisco HyperFlex
- Limitations for Dell EMC VNX, VNXe/Unity
- Limitations for NetApp
- Requirements for Universal Storage API Integrated Systems
System Requirements

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots are supported for the following storage devices:

Storage Integration

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots are supported for the following storage devices:

Cisco HyperFlex (HX-Series/SpringPath)

- NFS connectivity only
- HyperFlex 2.0 or later (Backup from Storage Snapshots, Full Integration mode)
- Basic authentication is not supported for SSO users in HyperFlex starting from version 3.0

Dell EMC VNX, VNX2, VNXe and Unity

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Dell EMC VNXe/Unity OE versions 3.x up to 5.0

Fujitsu ETERNUS DX/AF series

- Fibre Channel (FC) or iSCSI connectivity
- ETERNUS DX series: DX60 S4, DX100 S4, DX200 S4, DX500 S4, DX600 S4
- ETERNUS AF series: AF250 S2, AF650 S2
- Storage firmware version V10L86-0000 or later

HPE 3PAR StoreServ

- Fibre Channel (FC) or iSCSI connectivity
- 3PAR OS versions 3.1.2 up to 3.3.1 MU2
- iSCSI VLAN tags are supported
- Virtual Domains are supported

HPE Nimble Storage AF-Series, HF-Series and CS-Series

- Fibre Channel (FC) or iSCSI connectivity
- Nimble OS 2.3 or later
- HPE Nimble synchronous replication is not supported
HPE StoreVirtual (LeftHand / P4000 series) and StoreVirtual VSA

- iSCSI connectivity only
- LeftHand OS versions 9.5 up to 12.7
- HPE SV3200 (LeftHand OS version 13) is not supported

Huawei OceanStor

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Huawei OceanStor V3 and F V3 Series with software version V300R006 or later
- Huawei OceanStor Dorado V3 Series with software version V300R001 or later
- Huawei OceanStor V5 and F V5 Series with software version V500R007 or later

IBM Spectrum Virtualize (IBM Storwize, IBM SVC, Lenovo Storage V series)

- Fibre Channel (FC) or iSCSI connectivity
- IBM Spectrum Virtualize OS 7.6 or later

INFINIDAT Infinibox F-series

- NFS, Fibre Channel (FC) or iSCSI connectivity
- InfiniBox 3.0 or later

You must add to the backup infrastructure only one of the two InfiniBox storage arrays for which Active/Active Replication is configured, or exclude the replicating volumes on one of these arrays from rescan. For details on how to exclude volumes from rescan, see Rescanning Storage Systems.

NetApp FAS/AFF, FlexArray (V-Series), ONTAP Edge/Select/Cloud VSA and FAS OEM (IBM N series and Lenovo DM series)

- NFS, Fibre Channel, iSCSI
- ONTAP 7-mode versions 8.2 up to 9.5
- ONTAP cluster-mode versions 8.3 up to 9.5
- MetroCluster is supported
- ONTAP features application-aware data management and SVM-DR are not supported
- NetApp Synchronous SnapMirror is not supported

NetApp SolidFire/HCI

- iSCSI connectivity
- NetApp SolidFire support requires Element OS 9.0 or later
- NetApp HCI support requires Element OS 10.0 or later
Pure Storage FlashArray

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Purity 4.8 or later
- Purity ActiveCluster is supported

Western Digital IntelliFlash

- NFS, Fibre Channel (FC) or iSCSI connectivity
- Western Digital IntelliFlash 3.9.2 or later
General Limitations

The following limitations apply to all storage systems supported by Veeam Backup & Replication:

- **Backup infrastructure**
- **Backup from Storage Snapshots**
- **Snapshot Orchestration and Backup from Storage Snapshots with Snapshot Retention**
- **Veeam Explorer for Storage Snapshots**

Backup Infrastructure

Backup infrastructure for storage snapshots has the following limitations.

- CHAP authentication is not supported for storage systems working over iSCSI.
- SAS connections are not supported.
- Veeam Backup & Replication does not display volumes with the ‘VeeamAUX’ prefix in the storage hierarchy. Such volumes are used for service purposes and are filtered out.
- [For Huawei OceanStor] Huawei UltraPath software for storage connection redundancy and load balancing is not supported. It is recommended to use the Microsoft Multipath I/O (MPIO) feature instead.

Backup from Storage Snapshots

Backup from Storage Snapshots has the following limitations.

- Backup from Storage Snapshots does not support vRDM disks. vRDM disks are skipped from processing.
- Backup from Storage Snapshots cannot be used for VMs whose disks are located on VVol datastores.
- When configuring in VMware vSphere an NFS datastore that will host VM disks, you must specify the IP address of the NFS server rather than its DNS name. Otherwise, Veeam Backup & Replication may not be able to perform Backup from Storage Snapshots for VMs whose disks reside on this NFS datastore.
  
  For details on how to configure an NFS datastore in VMware vSphere, see VMware Docs.
- Backup from Storage Snapshots cannot be used to back up VM templates.
- For storage systems working over NFS:
  
  - VMs that you plan to back up or replicate must not have VMware vSphere snapshots. VMs with snapshots are skipped from processing.
  - If you enable the Enable VMware tools quiescence option in the job settings, Veeam Backup & Replication will not use Backup from Storage Snapshots to process running Microsoft Windows VMs that have VMware Tools installed.
Snapshot Orchestration and Backup from Storage Snapshots with Snapshot Retention

Snapshot jobs (snapshot-only jobs and backup jobs with storage snapshot retention) have the following limitations.

- If you remove or re-add a storage array that is already associated with a snapshot job, Veeam Backup & Replication will restart the retention cycle. You will need to manually remove old snapshots that are no longer needed.
- You cannot configure a job to create storage snapshots on arrays of different storage vendors.
- [For HPE 3PAR Peer Persistence] You can use backup jobs to create a snapshot chain either on a primary or on a secondary storage array, but you cannot configure snapshot creation on both storage arrays at the same time.
- For IBM Spectrum Virtualize:
  - When you add IBM Spectrum Virtualize storage systems with HyperSwap function to the backup infrastructure, Veeam Backup & Replication, by default, works with primary storage volumes. If you want to select secondary storage volumes as a data source for backup, use registry keys. For more information, contact Veeam Support Team.
  - You can use backup jobs to create a snapshot chain either on a primary or on a secondary storage array, but you cannot configure snapshot creation on both storage arrays at the same time.
- For snapshot-only jobs:
  - If a VM added to the job has several disks that reside on the same volume, you cannot exclude specific VM disks from the backup as Veeam Backup & Replication creates snapshots at the volume level.
  - Veeam Backup & Replication does not support the following guest processing options for snapshot-only jobs: Microsoft SQL Server and Oracle log backup and guest file indexing.
  - You cannot perform backup of VMs residing on a VMware datastore that comprises several LUNs.

Veeam Explorer for Storage Snapshots

Veeam Explorer for Storage Snapshots has the following limitations.

- During restore of VM guest OS files from storage snapshots, data is transferred over LAN through the Network Block Device protocol (NBD). Therefore, restore performance may not be optimal.
- You cannot perform any kind of restore operation (Instant VM Recovery, VM guest OS files restore and application items restore) when a VMware datastore comprises several LUNs.
- Veeam Explorer for Storage Snapshots does not support VMs whose disks are located on VVol datastores.
• You can restore data of a VM whose disks are hosted on different VMware datastores. However, if you restore from native storage snapshots or snapshots that were created with earlier versions of Veeam Backup & Replication, mind the following:
  o The restored VM will have only those VM disks that are hosted on the same datastore as the VMX file.
  o You will be able to restore VM guest OS files or application items only from those VM disks that are hosted on the same datastore as the VMX file.
  o You will not be able to restore VM disks that contain the absolute path in the VMX file.
  o [For HPE Nimble and NetApp] You will not be able to perform Instant VM Recovery and restore VM guest OS files to the original location from snapshots on secondary storage arrays.

To overcome these limitations, you must restore from storage snapshots created with the current version of Veeam Backup & Replication.

• If you remove or re-add a storage array to the backup infrastructure, you will be able to restore data only from those VM disks that are hosted on the same datastore as the VMX file.

• You cannot restore data of a VM whose disks are hosted on storage systems of different storage vendors.

• Multi-OS file-level restore for encrypted VMs is not supported.

• You cannot restore files directly to the original location from backups of BSD, Mac and Solaris VMs. You cannot restore files directly to the original location from NSS filesystems. Use the Copy to option instead.

• If the original VM is removed from vSphere infrastructure or migrated to another datastore, you will not be able to perform VM guest OS files restore to the original location.
Limitations for Cisco HyperFlex

If you plan to perform backup and replication from Cisco HyperFlex storage snapshots, consider the following limitations:

- VMs must be hosted on the supported Cisco HyperFlex system. For more information, see System Requirements.

- Veeam Backup & Replication 9.5 Update 2 or later must be installed on the backup server. For more information, see Integration Modes.

- Currently Veeam Backup & Replication does not support scenarios where several Cisco HyperFlex systems are registered under different vCenter Servers. It is recommended that you back up VMs of each vCenter Server instance using a separate Veeam backup server.

- VMs must not have VMware vSphere snapshots.
  During backup or replication, Veeam Backup & Replication fails to trigger Cisco HyperFlex snapshots on VMs that already have VMware vSphere snapshots. You can instruct Veeam Backup & Replication to process these VMs in the regular data processing mode. To do this, enable the Failover to standard backup option in job settings.

- Disks of a processed VM must be hosted on the same Cisco HyperFlex NFS store. If some VM disks are hosted on an NFS store other than the store where the VM configuration file resides, such VM will be processed in the regular backup mode.

- The Limit processed VM count per storage snapshots to N option is not applicable to Cisco HyperFlex since snapshots for VMs hosted on Cisco HyperFlex are created at the VM level, not volume level.
Limitations for Dell EMC VNX, VNXe/Unity

If you plan to perform backup and restore from Dell EMC storage snapshots, consider the following limitations:

- Dell EMC VNX Block
- Dell EMC VNX File
- Dell EMC VNXe

Dell EMC VNX Block

The following limitations apply to Dell EMC VNX Block storage systems:

- Veeam Backup & Replication supports LUNs that reside on Storage Pools.
- To take LUN snapshots, Veeam Backup & Replication uses the VNX snapshot technology. Make sure that you have a license that covers this technology. The SnapView snapshot technology is not supported.

Dell EMC VNX File

The following limitations apply to Dell EMC VNX File storage systems:

- A read-only checkpoint can have only 1 writable snapshot. If a read-only checkpoint already has a writable snapshot, Veeam Backup & Replication uses this writable snapshot for restore.
- Writable snapshots are not detected by the storage rescan process and are not displayed in the storage system hierarchy.

Dell EMC VNXe

The following limitations apply to Dell EMC VNXe storage systems:

- In Dell EMC VNXe, you cannot export more than 1 storage snapshot for a LUN or LUN group concurrently. For this reason, Veeam Backup & Replication can perform only one task that uses storage snapshots at the same time.
- In Veeam Backup & Replication, tasks have the following priority levels (starting with the highest priority): restore task > backup job > rescan task. If you start several jobs or tasks that use storage snapshots, Veeam Backup & Replication will check what priority tasks have and perform the following actions:
  - If a LUN snapshot is exported for storage rescan and you start a backup job or restore task at the same time, the rescan process will fail.
  - If a LUN snapshot is exported for a backup job and you start another backup job at the same time, the second backup job will be waiting until the first backup job is finished.
  - If a LUN snapshot is exported for a restore task and you start a backup job at the same time, the backup job will fail (or failover to the regular processing mode if corresponding settings are enabled in the backup job).
  - If a LUN snapshot is exported for a backup job and you start a restore task at the same time, the restore task will be waiting until the backup job is finished.

This limitation does not apply to Dell EMC Unity storage systems.
Limitations for NetApp

If you plan to perform operations with NetApp Data ONTAP storage snapshots, consider the following limitations:

- Veeam Backup & Replication may fail to perform backup from secondary storage arrays if SVM/volumes have identical names between primary and secondary storage arrays.

- Depending on the protocol type and operating mode of the NetApp storage system, Veeam Backup & Replication uses different technologies to perform the following operations:
  - Storage system rescan
  - Backup from Storage Snapshots
  - Restore from storage snapshots

You may need to install additional NetApp licenses. You need to install one license, even if several technologies can be used for snapshot clone creation.

Rescan of NetApp Storage Systems

cDot

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>FlexClone</th>
<th>SnapRestore</th>
<th>No License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Storage System</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI/FC</td>
<td>Possible (preferred)</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
<tr>
<td><strong>Secondary Storage System: NetApp SnapMirror and SnapVault</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI/FC</td>
<td>Possible</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>
NOTE:
During storage rescan, Veeam Backup & Replication adds its export rules for the storage. New rules are added at the beginning of the list, shifting existing rules down in the list.

Backup from Storage Snapshots

7-Mode

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Traditional LUN Cloning (no license)</th>
<th>FlexClone</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC/ISCSI</td>
<td>Possible</td>
<td>Recommended</td>
</tr>
<tr>
<td>NFS</td>
<td>Not needed</td>
<td>Not needed</td>
</tr>
</tbody>
</table>

**cDot**

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>FlexClone</th>
<th>SnapRestore</th>
<th>No License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Storage System</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI/FC</td>
<td>Possible (preferred)</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>

**Secondary Storage System: NetApp SnapMirror and SnapVault**

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>FlexClone</th>
<th>SnapRestore</th>
<th>No License</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI/FC</td>
<td>Possible (mandatory)</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>

NOTE:
During backup from storage snapshots, Veeam Backup & Replication adds its export rules for the storage. New rules are added at the beginning of the list, shifting existing rules down in the list.

Traditional LUN Cloning

For NetApp storage systems that do not have a FlexClone license installed, Veeam Backup & Replication uses the NetApp traditional LUN cloning technology.

Traditional LUN clones are created with the help of a backing snapshot.

1. Veeam Backup & Replication creates a backing snapshot for a LUN holding VM data. The backing snapshot is a snapshot of a volume where the LUN is located. The backing snapshot acts as a helper, or medium, for the LUN clone. It contains a momentarily image of the LUN and captures the exact state of the LUN at the necessary point in time.
2. After that, Veeam Backup & Replication creates a LUN clone.

The LUN clone bases on the backing snapshot and shares its data with the backing snapshot. Veeam Backup & Replication cannot delete the backing snapshot before the LUN clone is removed. Deletion of the backing snapshot will corrupt the LUN clone.

In case of traditional LUN cloning, backing snapshots created by Veeam Backup & Replication may be locked and may fail to be deleted automatically with cleanup operations. This can happen, for example, if you schedule the NetApp storage system to create daily volume snapshots, and the scheduled operation begins before Veeam Backup & Replication deletes the backing snapshot that was used for backup or replication.

In this situation, the created backing snapshot will become a part of the snapshot chain. The scheduled snapshot and all subsequent snapshots will reference this snapshot, and Veeam Backup & Replication will be unable to remove it. As a result, your retention policy for scheduled snapshots may be disrupted.

To avoid this situation, it is recommended that you install a FlexClone license on the NetApp storage system. In this case, Veeam Backup & Replication will use the FlexClone technology for LUN cloning.

**FlexClone**

The FlexClone technology lets you create a transparent, space-efficient copy of a LUN. FlexClones are created in seconds and require little space on the storage. Unlike traditional LUN clones, FlexClones are independent and do not cause any problems with volume snapshot deletion.

For Backup from Storage Snapshots, Veeam Backup & Replication creates a FlexClone in the following way:

1. Veeam Backup & Replication creates a temporary snapshot of a volume hosting a LUN to capture the momentary state of this LUN.
2. After that, Veeam Backup & Replication creates a LUN clone.
This temporary volume snapshot is used as a base for a FlexClone. However, the base snapshot is not tied to the FlexClone, as a backing snapshot in traditional LUN cloning. Veeam Backup & Replication can delete it without any impact for the FlexClone at any time.

**SnapRestore**

For NetApp storage systems that work in the cDot operating mode and have a SnapRestore license installed, Veeam Backup & Replication can use the NetApp SnapRestore technology for Backup from Storage Snapshots.

Veeam Backup & Replication creates a storage snapshot in the following way:

1. Veeam Backup & Replication creates a snapshot of a volume holding VM data.
2. Veeam Backup & Replication creates a LUN clone via SnapRestore.

**NFS Protocol**

If the NetApp storage system operates over NFS, you do not have to install any additional licenses to use Backup from Storage Snapshots.

For Backup from Storage Snapshots, Veeam Backup & Replication creates a snapshot of a volume on which the NFS share with VM data resides. The created volume snapshot is used as a source of data. Veeam Backup & Replication starts its native NFS agent on the backup proxy and uses this agent to read data from the cloned NFS share on the volume snapshot.
## Restore from Storage Snapshots

### 7-Mode

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>Traditional LUN Cloning (No License)</th>
<th>FlexClone</th>
<th>SnapRestore</th>
<th>NDMP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Only one license is required</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC/iSCSI</td>
<td>Possible</td>
<td>Recommended</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Not possible</td>
<td>Recommended</td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
</tr>
<tr>
<td>FC/iSCSI SnapMirror</td>
<td>Not used</td>
<td>Mandatory</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>FC/iSCSI SnapVault</td>
<td>Used for restore</td>
<td>Mandatory (used for rescan*)</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS SnapMirror</td>
<td>Not possible</td>
<td>Recommended</td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
</tr>
<tr>
<td><strong>Several licenses are used</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS SnapVault</td>
<td>Not possible</td>
<td></td>
<td>For file-level restore and application item restore, Veeam Backup &amp; Replication can use FlexClone**. For VM restore, Veeam Backup &amp; Replication can use SnapRestore or NDMP (check columns on the right).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
<td>Limited usage. Veeam Backup &amp; Replication transports all data before Instant VM Recovery, file-level restore or application item restore starts.***</td>
</tr>
</tbody>
</table>

* Not used for restore operations due to NetApp SnapVault limitations.
** Can be used only for file-level restore. To enable restore, you can use registry keys. For more information, contact Veeam Support Team.
*** Veeam Backup & Replication copies VM files from the /vol/volname/VMFolder/ folder from the snapshot to the /vol/vvolname/Veeam_Restore_VMname/VMFolder/ folder, and restore wizards work with copied files.
cDot

<table>
<thead>
<tr>
<th>Storage Type</th>
<th>FlexClone</th>
<th>SnapRestore</th>
<th>No License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Storage System</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI/FC</td>
<td>Possible (preferred)</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible</td>
<td>Possible</td>
<td>Not possible</td>
</tr>
<tr>
<td><strong>Secondary Storage System: NetApp SnapMirror and SnapVault</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iSCSI/FC</td>
<td>Possible (mandatory)</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
<tr>
<td>NFS</td>
<td>Possible (mandatory)</td>
<td>Not possible</td>
<td>Not possible</td>
</tr>
</tbody>
</table>

**Traditional LUN Cloning**

For NetApp storage systems that do not have the FlexClone license installed, Veeam Backup & Replication uses the NetApp traditional LUN cloning technology.

During restore from storage snapshots, Veeam Backup & Replication creates a LUN clone. The storage snapshot from which you want to restore data is used as a backing copy. The LUN clone is then mounted to an ESXi host, and you can restore VM data from it.

**FlexClone**

For NetApp storage systems that have a FlexClone license installed, Veeam Backup & Replication uses the NetApp FlexClone technology for restore from storage snapshots.
During restore from storage snapshots, Veeam Backup & Replication creates a FlexClone of a LUN. The storage snapshot from which you want to restore data is used as a base copy. The FlexClone is then mounted to an ESXi host, and you can restore the necessary VM data from it.

**SnapRestore**

For NetApp storage systems that have a SnapRestore license installed, Veeam Backup & Replication uses the NetApp SnapRestore technology for restore from storage snapshots.

When you restore data from storage snapshot, Veeam Backup & Replication triggers NetApp to create a clone of a LUN via SnapRestore. To do this, NetApp restores LUN data to a new location on the volume where the original LUN is located. As a result, you have a read-write copy of the LUN holding VM data, and can use this copy for restore operations.

**NFS Protocol**

When you perform restore from storage snapshot on NetApp storage systems working over the NFS protocol, Veeam Backup & Replication triggers NetApp to clone an NFS share that holds VM data. NetApp creates a copy of the NFS share and places this copy on the same volume where the original NFS share is located. This copy is used as a data source for restore operations.

After a copy of the NFS share is created, Veeam Backup & Replication mounts the NFS share copy to an ESX(i) host as a new datastore, and you can restore VM data from the mounted NFS share copy.

If you have several VMs that reside on the same storage snapshot, Veeam Backup & Replication will create only one NFS datastore per snapshot. During restore, VMs from the same snapshot are copied to the same folder on the volume where the original NFS share is located. When you start the restore process for the first VM on the storage snapshot, the folder is presented as a datastore to an ESX(i) host. After you finish the restore process for the last VM on the storage snapshot, the folder is unmounted from the ESX(i) host.

Depending on the operation mode of the NetApp storage system, Veeam Backup & Replication uses different technologies to create a clone of an NFS share.
7-mode
If the NetApp storage system operates in the 7-mode, you must have a FlexClone or SnapRestore license installed, or the NDMP protocol enabled.

Veeam Backup & Replication uses the following technologies for LUN clone creation:

- If you have a FlexClone license installed, Veeam Backup & Replication uses the FlexClone technology.
- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.

If neither FlexClone nor SnapRestore license is installed, Veeam Backup & Replication uses the NDMP protocol. If the NDMP protocol is not enabled, VM data restore will fail.

**IMPORTANT!**
[For Instant VM Recovery] Veeam Backup & Replication performs actual Instant VM Recovery only if a FlexClone license is installed. If the SnapRestore license is installed or the NDMP protocol is enabled, Veeam Backup & Replication performs entire VM restore instead of Instant VM Recovery. As a result, the restore process takes more time.

C-mode
If the NetApp storage system operates in the C-mode, you must have a FlexClone or SnapRestore license installed.

- If you have a FlexClone license installed, Veeam Backup & Replication uses the FlexClone technology.
- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.

If neither FlexClone nor SnapRestore license is installed, VM data restore will fail.

**Restore from SnapVault**

7-mode
If the NetApp storage system operates in the 7-mode, you must have a FlexClone or SnapRestore license installed, or the NDMP protocol enabled.

- If you have a SnapRestore license installed, Veeam Backup & Replication uses the SnapRestore technology.
• If a SnapRestore license is not installed, Veeam Backup & Replication uses the NDMP protocol. If the NDMP protocol is not enabled, VM data restore will fail.

**IMPORTANT!**

[For Instant VM Recovery] If you restore data from NetApp SnapVault, Veeam Backup & Replication performs entire VM restore instead of Instant VM Recovery. As a result, the restore process takes more time.

**C-mode**

If the NetApp storage system operates in the C-mode, you must have a FlexClone license installed. In the opposite case, VM data restore will fail.
Requirements for Universal Storage API Integrated Systems

Before you add a Universal Storage API integrated system to your backup infrastructure, check the following prerequisites.

- Make sure that you have installed the storage system plug-in. For more information, see Installing Storage System Plug-Ins.

- For Fujitsu ETERNUS storage systems:
  - Veeam Backup & Replication 9.5 Update 4a or later must be installed on the backup server.
  - You must obtain and install the Veeam Storage Integration license on the Fujitsu ETERNUS storage system.
    The Veeam Storage Integration license is free of charge. You can obtain the license from the Fujitsu website.

- For Western Digital IntelliFlash storage systems, Veeam Backup & Replication 9.5 Update 4b or later must be installed on the backup server.
Required Permissions

To perform data protection and disaster recovery operations with storage snapshots, a user account must have a set of permissions on the relevant storage system.

In This Section

- NetApp Data ONTAP Permissions
- NetApp SolidFire/HCI Permissions
NetApp Data ONTAP Permissions

A user account that you plan to use for working with the NetApp Data ONTAP storage system must have the following permissions:

7-Mode

- login-http-admin
- api-system-*
- api-license-* (api-license-list-info)
- api-volume-*
- api-net-*
- api-options-*
- api-vfiler-*
- api-qtree-*
- api-nfs-*
- api-snapshot-*
- api-lun-*
- api-iscsi-*
- api-feature-*
- api-registry-*
- cli-options
- api-fcp-*
- api-file-*
- api-igroup-*
- api-clone-*
- api-snapvault-*
- api-snapmirror-*
- api-cf-*
## cDot

<table>
<thead>
<tr>
<th>Command/Directory</th>
<th>Access/Query Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT</td>
<td>readonly</td>
</tr>
<tr>
<td>cluster</td>
<td>readonly</td>
</tr>
<tr>
<td>metrocluster</td>
<td>readonly</td>
</tr>
<tr>
<td>fcp</td>
<td>readonly</td>
</tr>
<tr>
<td>file</td>
<td>readonly</td>
</tr>
<tr>
<td>igroup</td>
<td>all</td>
</tr>
<tr>
<td>iscsi</td>
<td>all</td>
</tr>
<tr>
<td>network</td>
<td>readonly</td>
</tr>
<tr>
<td>node</td>
<td>readonly</td>
</tr>
<tr>
<td>security</td>
<td>readonly</td>
</tr>
<tr>
<td>security login</td>
<td>readonly</td>
</tr>
<tr>
<td>set</td>
<td>readonly</td>
</tr>
<tr>
<td>snapmirror</td>
<td>all</td>
</tr>
<tr>
<td>system</td>
<td>readonly</td>
</tr>
<tr>
<td>version</td>
<td>readonly</td>
</tr>
<tr>
<td>qtree</td>
<td>readonly</td>
</tr>
<tr>
<td>lun</td>
<td>all</td>
</tr>
<tr>
<td>nfs</td>
<td>all</td>
</tr>
<tr>
<td>snapshot</td>
<td>all</td>
</tr>
<tr>
<td>volume</td>
<td>all</td>
</tr>
<tr>
<td>vs server</td>
<td>all</td>
</tr>
</tbody>
</table>
NetApp SolidFire/HCI Permissions

A user account that you plan to use for working with the NetApp SolidFire/HCI storage system must have the following permissions:

- Volumes
- Cluster Admins